

On Sequences, Rational Functions and Decomposition

Graham H. Norton*

April 8, 2015

Abstract

It is classical that well-known identities and properties of partial quotients furnish rational approximation in $\mathbb{F}[[x^{-1}]]$. For a rational function, this is the extended Euclidean algorithm in $\mathbb{F}[x]$. Berlekamp's heuristic solution of the 'key equation' essentially approximates an element of $\mathbb{F}[x]$ with constant term 1 via a quotient of reciprocals, and his solutions satisfy a number of identities. In earlier papers we gave a solution of an analogous problem using $D[x^{-1}, x]$, D a commutative domain.

The linear complexity (of a finite initial subsequence) of an infinite sequence over \mathbb{F} has been related to the degrees of its partial quotients by Mills, Cheng, Niederreiter and others. We use first principles and induction to relate these linear complexities to the degrees of its partial quotients.

Berlekamp has also described the set of solutions of the key equation. We define a pairing of minimal solutions and a 'minimal system' of a finite sequence over D . Examples are classical approximation in $\mathbb{F}[[x^{-1}]]$ and approximation using $D[x^{-1}, x]$. We use minimal systems to generalise results of Massey and Niederreiter to arbitrary solutions, including numerators. This includes explicit and unique decomposition of both parts of a solution into a sum of (polynomial) multiples of solutions with minimal degree denominators. The unique multipliers also satisfy degree constraints.

We give several applications to gcd's of sequence polynomials and relate partial-quotient solutions to solutions derived using $\mathbb{F}[x^{-1}, x]$. We give a precise count of the number of solutions when the field is finite. Our final application concerns when the first component of a minimal solution vanishes at some scalar; a simple modification of our approach gives a new solution, the first component of which does not vanish at the scalar and which has minimal degree. We also describe the corresponding set of solutions. This simplifies and generalises work of Salagean.

We conclude that numerators (or second components) of solutions can play a significant role in proofs of properties of denominators (or first components) and that they enjoy similar properties.

Keywords Berlekamp-Massey algorithm, continued fraction, key equation, Laurent series, linear recurrence, minimal polynomial, partial quotient, rational function.

*School of Mathematics and Physics, University of Queensland, Brisbane, Queensland 4072, Australia (email: ghn@maths.uq.edu.au).

Contents

1	Introduction	3
1.1	Background	3
1.2	Overview	3
1.3	In More Detail	4
1.4	Standard Notation	6
1.5	Guide to Additional Notation	7
2	Sequence Basics	8
2.1	Rational Approximation and Solutions	8
2.2	Linear Recurring Sequences	8
2.3	Annihilating Polynomials and Solutions	9
2.4	First Examples and the Key Lemma 2.6	10
2.5	Linear Complexity and Minimal Solutions	11
3	Minimal Solutions via Partial Quotients	12
3.1	Continued Fractions	12
3.2	Geometric Sequences	15
3.3	Essential Sequences and the General Case	15
4	An Inductive Construction of Minimal Solutions	18
4.1	Pseudo-Geometric Sequences	18
4.2	Essential Sequences or, a Tale of Two Triples	19
4.3	The Inductive Theorem and the Corresponding Algorithm	20
4.4	A Worst-Case Analysis	24
4.5	An Identity for μ and μ'	25
5	Decomposition	26
5.1	A Pairing	26
5.2	Geometric Sequences. II	26
5.2.1	Annihilating Polynomials	27
5.2.2	Solutions	28
5.3	Essential Sequences. II	29
5.3.1	Annihilating Polynomials	29
5.3.2	Solutions	31
6	Some Applications of Decomposition	32
6.1	Sequences over a Field	32
6.2	Non-Vanishing Annihilating Polynomials	33

1 Introduction

1.1 Background

Let \mathbb{F} be a field. Approximating the generating function $S_1x^{-1} + S_2x^{-2} + \dots \in x^{-1}\mathbb{F}[[x^{-1}]]$ by rational functions $q_2^{(i)}/q_1^{(i)}$ (where $i \geq 0$) is well-known; $q_1^{(i)}, q_2^{(i)}$ are known as its partial quotients or rational convergents. An important identity is

$$q_2^{(i)}q_1^{(i-1)} - q_1^{(i)}q_2^{(i-1)} = (-1)^{i-1}. \quad (1)$$

Obtaining partial quotients uses division in the field of Laurent series in x^{-1} , written $\mathbb{F}((x^{-1}))$. When the above sum is a rational function, this is the extended Euclidean algorithm. See also [8] for connections with linear recurring sequences.

A second example is Berlekamp's iterative solutions $\omega^{(i)}/\sigma^{(i)}$ of the 'key equation', where $0 \leq i \leq n$, [1, Section 7]. (The integer n is related to a decoding problem.) It is essentially rational approximation of $1 + s_1x + \dots + s_nx^n \in \mathbb{F}[x]$ using reciprocals of polynomials. It uses 'auxiliary solutions' $\gamma^{(i)}/\tau^{(i)}$ which satisfy $\omega^{(i)}\tau^{(i)} - \sigma^{(i)}\gamma^{(i)} = x^i$, [1, Theorem 7.42]. The set of solutions was discussed in [1, Theorems 7.43, 7.44].

A simplification of Berlekamp's algorithm appeared in [7, Algorithm 1]. This interprets $\sigma^{(n)}$ as a 'connection polynomial of a minimal-length linear-feedback shift register (LFSR) which generates $s = s_1, \dots, s_n$ '. It is known as the Berlekamp-Massey algorithm. The minimal length is called the 'linear complexity' L_n of s . The set of connection polynomials for all LFSR's of length L_n which generate s was given in [7, Theorem 3].

Connections between these two types of rational approximation e.g. between the linear complexity of S_1, \dots, S_n and the degrees of the denominators $q_1^{(i)}$ have been discussed in [2], [8] and [15], which depend on [1]. In [9, Theorem 1] this was done independently of [1] and [7].

A third example appeared in [11]. Our goal was a faithful redevelopment and extension of [7]; we were unaware of [9] and Macaulay's inverse systems, see e.g. [10]. We discussed rational approximation of $s_0 + \dots + s_{1-n}x^{1-n} \in D[x^{-1}]$ using Laurent polynomials $D[x^{-1}, x]$, where D is a commutative domain. We write our solution as $\mu = (\mu_1, \mu_2)$ and call μ_1 a 'minimal polynomial' of s . The linear complexity L_n of s is the degree of μ_1 and the reciprocal of μ_1 is a connection polynomial of an LFSR generating s , [13]. When D is a field, our approach has applications to the above decoding problem and to control theory, see for instance [12, Section 8] and [11, Example 4.9].

1.2 Overview

Our overall goal is to unify and extend some results in the literature related to the rational approximation of generating functions of infinite and finite sequences. In our approach, numerators play a significant role.

We revisit [9, Theorem 1], which has two parts. We give an inductive proof of the first part on linear complexity and partial quotients. Our proof is from first principles, using the basic definitions for finite sequences from [11]. We also prove the converse.

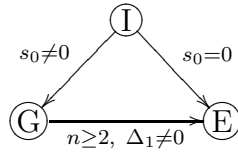
We also derive an analogue of Identity (1) for our minimal solutions, Proposition 4.20. This enables us to 'decompose' solutions and determine the set of all solutions for a finite sequence over D whenever we have a 'minimal system' for s . Partial quotients (with $D = \mathbb{F}$) also provide a minimal system. In this way we generalise the second part of [9, Theorem 1] to all solutions. We conclude with some applications of decomposition.

Note to the reader: we consider the partial quotients for an infinite sequence over a field only; we have not extended [2] and [9] to commutative domains. In some situations, we apply our results to finite sequences over a field e.g. Proposition 2.8, Proposition 4.14 on monic minimal polynomials and Corollaries 6.1 - 6.4. We have included a number of examples; some reappear intentionally in different guises as an expository aid and others are inductive bases for later theorems.

1.3 In More Detail

We begin with basic concepts for infinite sequences over \mathbb{F} , denoted S_0, S_{-1}, \dots and finite sequences over D , denoted s_0, \dots, s_{1-n} where $n \geq 1$; this indexing agrees with Macaulay's inverse systems in [10] and with finite sequences in [11].

We can regard finite sequences as trivial ($s = 0, \dots, 0$), geometric or 'essential', Proposition 2.10. Geometric sequences are those of high school, defined by $s_0 \neq 0$ and a common ratio. Equivalently, they satisfy $L_n = \dots = L_1 = 1$. 'Essential' sequences on the other hand satisfy $L_n > L_1 \geq 0$ and predominate: geometric sequences may become essential on adding a term, but never the reverse, see Proposition 2.11. We summarise this using a state diagram ('I' is the start state, 'G' denotes 'geometric' and 'E' denotes 'essential'; we have suppressed transitions between the same state):

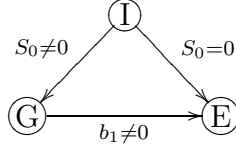


where $s \neq 0, \dots, 0$ and Δ_1 denotes a 'discrepancy'. Unfortunately this subdivision of sequences does not appear in [7], which renders the Berlekamp-Massey algorithm harder to understand. If $n \geq 2$ and $s = s_0, \dots, s_{1-n}$ is essential then

$$n' = \max\{1 \leq j < n : L_j < L_n\}$$

is a well-defined integer, $1 \leq n' < n$, and we have the important subsequence $s_0, \dots, s_{1-n'}$.

We next discuss partial quotients (when $S \neq 0, 0, \dots$) as these are classical and less detailed, being based on division in $\mathbb{F}((x^{-1}))$. First we treat the base cases in Propositions 3.4, 3.6. We obtain an inductive proof of the first part of [9, Theorem 1] and its converse, Theorem 3.7. This gives a similar state diagram for S , Proposition 3.8:



Then we revisit [11], restricting to geometric and essential sequences over D only. This new approach is simpler, see Theorem 4.9; the corresponding Algorithm 4.12 is valid for all sequences and is virtually identical to [11, Algorithm 4.6]; we compute $\mu = (\mu_1, \mu_2)$ rather than $(\mu_1, x\mu_2)$. (Apart from Lemmas 4.2 and 4.7 — which the interested reader may verify — this paper is independent of [11].)

For sequences over a field, there is a 'normalised Algorithm 4.12' which computes a monic μ_1 , Proposition 4.14. This has been implemented in COCOA, [3]. We also prove an identity for the sum of the linear complexities of s . This seems to be new and gives a simple analysis of Algorithm 4.12, see Proposition 4.17.

We use Algorithm 4.12 to define an element $\nabla_s \in D \setminus \{0\}$ and prove the identity

$$\mu_2 \mu'_1 - \mu_1 \mu'_2 = \nabla_s \quad (2)$$

where μ' is either $(1, 0)$ or a minimal solution for $s_0, \dots, s_{1-n'}$. This is our analogue of Identity (1) and the identity of Berlekamp mentioned above. Identity (2) easily implies that for any $f = (f_1, f_2) \in D[x]^2$

$$\nabla_s f_1 = m' \mu_1 - m \mu'_1 \quad (3)$$

where $m = f_2 \mu_1 - f_1 \mu_2$ and $m' = f_2 \mu'_1 - f_1 \mu'_2$. This is a special case of a pairing $D[x]^2 \times D[x]^2 \rightarrow D[x]$ defined by μ and μ' .

In fact, essential sequences exhibit a 'minimal system', a stronger property than (3), Definition 5.8. We show that if f is a solution and we have a minimal system, then these multipliers (i) satisfy degree bounds and (ii) are unique when the degree of f_1 is at most n ; in this case we call (3) a 'decomposition' of $\nabla_s f_1$. And ∇f_2 satisfies a similar identity with the same multipliers i.e. we have a decomposition of $\nabla_s f$. This yields the required description of all solutions when we have a minimal system, see Corollary 5.15. Partial quotients also exhibit a minimal system. In this way, we generalise the second part of [9, Theorem 1]. It also strengthens [11, Theorem 4.17] and has a simpler proof.

There are lacunae for geometric sequences as they do not have a minimal system. However this does not embarrass us, as using $(q_1^{(0)}, q_2^{(0)}) = (\mu'_1, \mu'_2) = (1, 0)$ enables us to give alternative proofs in both the partial quotient and finite sequence contexts. Secondly, over a domain D , we have to work with 'pseudo-geometric' sequences as the leading coefficient of μ_1 may not be a unit of D . As these sequences are inherently simpler and easier to treat than the essential ones, we always discuss them first.

We have included some applications. We show that for a sequence s over a field and solution (f_1, f_2) such that the degree of f_1 is at most $n - L_n$ (i) $\gcd(f_1, f_2) = 1$ implies

that f is a minimal solution and (ii) the multipliers of Identity (3) satisfy $\gcd(m, m') = \gcd(f_1, f_2)$. We apply (i) to linear recurring sequences. We relate our minimal polynomials and partial quotients, Corollary 6.2. We also give a precise count of the number of solutions when $|\mathbb{F}| < \infty$.

For our final application, we revisit some work of Salagean, [14]. Let $a \in D$ be arbitrary and suppose that $\mu_1(a) = 0$. We show that Identity (3) implies that the lower bound for the degree of an annihilating polynomial of s which does not vanish at a is $M = L_n + \max\{n + 1 - 2L_n, 0\}$. We exhibit a solution of minimal degree

$$x^M \mu - \mu'$$

— the polynomial $x^M \mu_1 - \mu'_1$ does not vanish at a by Identity (3). Algorithm 6.8 is a one-line extension of Algorithm 4.12 and is simpler than [14, Algorithm 3.2]. We also derive the corresponding numerator. In fact the bound in Theorem 6.7 and the set of minimal polynomials in Corollary 6.12 were stated without proof in [14] and used to justify Algorithm 3.2, *loc. cit.*

We thank the anonymous referee for a number of useful comments and suggestions which improved the presentation, and also the members of *Projet Secret* at INRIA, Rocquencourt for their hospitality.

1.4 Standard Notation

For any set E containing 0, $E^\times = E \setminus \{0\}$ so that $\mathbb{N}^\times = \{1, 2, \dots\}$. As usual, $\sum_\emptyset = 0$.

Throughout the paper, D is a commutative domain with $1 \neq 0$ and $R = D[x]$. For any $a \in D^\times$ and $A \subseteq D$, $aA = \{ab : b \in A\}$. For $f \in R$, $|f|$ is the *degree* of $f \in R$, with $|0| = -\infty$; the usual rules for arithmetic involving $-\infty$ apply. If $f \in R^\times$, $\text{lc}(f)$ is the *leading coefficient* of f . We often write $f = x^k g + h$ if $f(x) = x^k g(x) + h(x)$ where $k \in \mathbb{N}$ and $g, h \in R$. For $f, g \in R$, their product is written fg and we regard R^2 as an R -module via $f(g, h) = (fg, fh)$.

A non-zero *formal negative Laurent series* over D is $L = \sum_{-\infty < i \leq k} L_i x^i \in D((x^{-1}))$ where $k \in \mathbb{Z}$, $L_i \in D$ and $L_k \neq 0$; we write

$$v(L) = k \quad \text{and} \quad [L] = \sum_{i=1}^k L_i x^i \in xR$$

i.e. $v : D((x^{-1})) \rightarrow \{-\infty\} \cup \mathbb{Z}$ is the *exponential valuation*, with $v(L) = -\infty \Leftrightarrow L = 0$; v coincides with $| \cdot |$ on R . It is elementary that $v(L \cdot M) = v(L) + v(M)$, $v(L + M) \leq \max\{v(L), v(M)\}$ and $v(L + M) = \max\{v(L), v(M)\}$ if $v(L) \neq v(M)$. We also write v for the restriction of v to $D[x^{-1}] \subset D((x^{-1}))$. We regard $D((x^{-1}))$ as $D[[x^{-1}]] + xR$ and use \cdot for multiplication in $D((x^{-1}))$.

We denote an arbitrary field by \mathbb{F} . For continued fractions in $\mathbb{F}[[x^{-1}]]$ we use $\text{Pol}(L) = \sum_{i=0}^{v(L)} L_i x^i \in \mathbb{F}[x]$. As usual, $\mathbb{F}(x) \subset \mathbb{F}((x^{-1}))$ is the subfield of rational functions over \mathbb{F} .

1.5 Guide to Additional Notation

We include a table of additional symbols used in the paper to aid the reader.

Symbol	Meaning
0^n	sequence of n zeroes
a, b, c	elements of D
a_i	$[a_1, a_2, \dots]$ is the continued fraction expansion of \underline{s} and $i \geq 1$
$\text{Ann}(s)$	set of annihilating polynomials of s
b_i	Laurent series in i^{th} iteration of partial quotient algorithm, $i \geq 0$
e, e_s	$n + 1 - 2L_n$
f, g	elements $(f_1, f_2), (g_1, g_2)$ of R^2
f_2	$[f_1 \cdot \underline{s}]/x$
$\langle f, g \rangle$	$f_2 g_1 - f_1 g_2 \in R$, the pairing of f and g
Id_S	ideal of characteristic polynomials of S
$L, L(s), L_n$	linear complexity of $s = s_0, \dots, s_{1-n}$
$L', L(s'), L_{n'}$	linear complexity of s' , s essential
m, m'	$\langle f, \mu \rangle, \langle f, \mu' \rangle$ respectively
$\text{MP}(s)$	set of minimal polynomials of s
n	a strictly positive integer
n'	the strictly positive integer $\max_{1 \leq j < n} \{j : L_j < L_n\}$, s essential
n_i	strictly positive integer $ q_1^{(i-1)} + q_1^{(i)} $ or ∞
∇	∇_s (non-zero product of discrepancies) or $(-1)^{i-1}$
$q^{(i)}$	i^{th} partial quotient $(q_1^{(i)}, q_2^{(i)})$, $i \geq 0$
s	finite sequence s_0, \dots, s_{1-n} over D
s, s_{-n}	$s_0, \dots, s_{1-n}, s_{-n}$
\underline{s}	$s_0 + s_{-1}x^{-1} + \dots + s_{1-n}x^{1-n}$
s'	the subsequence $s_0, \dots, s_{1-n'}$ of essential s
S	infinite sequence over \mathbb{F}
\underline{S}	$S_0 + S_{-1}x^{-1} + \dots$
$S n$	S_0, \dots, S_{1-n}
T_s	triple (n, μ_1, Δ_1) for s
T'_s	triple (n', μ'_1, Δ'_1) for s' , s essential
$\Delta_1 = \Delta(\mu_1; s, s_{-n})$	next discrepancy of $\mu_1 \in \text{MP}(s)$
Δ'_1	next discrepancy of μ'_1
λ	either μ or $q^{(i)}$, as used in Section 5
μ	minimal solution (μ_1, μ_2) for s from Theorem 4.9
μ_1	minimal polynomial of s from Theorem 4.9
μ'_1	1 if s is pseudo-geometric, or minimal polynomial of s'
ν	new minimal solution obtained from μ, μ'
ξ	solution with $\xi_1(a) \neq 0$ constructed in Section 6, $a \in D$
ϕ, ϕ', ψ	elements of R .

2 Sequence Basics

2.1 Rational Approximation and Solutions

Given an infinite sequence $S = S_0, S_{-1}, \dots$ over \mathbb{F} , rational approximation of the generating function of S and continued fractions is classical. Consider the following problem: for $n \geq 1$, find a rational function $x f_2/f_1 \in \mathbb{F}(x)$ with $|f_2| < |f_1|$ such that

$$(x f_2/f_1)_i = S_i \text{ for } 1 - n \leq i \leq 0 \quad (4)$$

and $|f_1|$ is minimal. Let $\underline{S} = \sum_{i \leq 0} S_i x^i \in \mathbb{F}[[x^{-1}]]$ be the *generating function* of S . We can rephrase (4) as: find $x f_2/f_1$ such that $v(\underline{S} - x f_2/f_1) \leq -n$ and $x f_2 = [f_1 \cdot \underline{S}]$. Multiplying by f_1 , we equivalently require (f_1, f_2) such that

$$v(f_1 \cdot \underline{S} - x f_2) \leq |f_1| - n \text{ and } x f_2 = [f_1 \cdot \underline{S}]. \quad (5)$$

Let $\{q_2^{(i)}/q_1^{(i)} : i \geq 0\}$ be the partial quotients of $x^{-1}\underline{S}$. In [9] (with $S = S_1, S_2, \dots$ and $\underline{S} = \sum_{i \geq 1} S_i x^{-i} \in x^{-1}\mathbb{F}[[x^{-1}]]$) Theorem 1, *loc. cit.* shows that

- (i) if $|q_1^{(i-1)}| + |q_1^{(i)}| \leq n < |q_1^{(i)}| + |q_1^{(i+1)}|$ then $(q_1^{(i)}, q_2^{(i)})$ solves (5);
- (ii) $q_1^{(i)}$ is an ' n^{th} minimal polynomial' of S , [9, p. 39];
- (iii) all n^{th} minimal polynomials of S can be expressed in terms of $q_1^{(i)}$ and $q_1^{(i-1)}$.

2.2 Linear Recurring Sequences

For an infinite sequence S over \mathbb{F} , we easily have $\underline{S} = x\psi/\varphi \in \mathbb{F}(x)$ for some $\psi \in \mathbb{F}[x]$ with $|\psi| < |\varphi| = d$ if and only if $(\varphi \cdot \underline{S})_i = 0$ for $i \leq 0$ and $x\psi = [\varphi \cdot \underline{S}]$. Now $(\varphi \cdot \underline{S})_i = \varphi_d S_{i-d} + \varphi_{d-1} S_{i-d+1} + \dots + \varphi_0 S_i$ so that $S_0, \dots, S_{1-d}, \varphi$ and the equation

$$S_{i-d} = -(\varphi_{d-1} S_{i-d+1} + \dots + \varphi_0 S_i)/\varphi_d \quad \text{for } i \leq 0 \quad (6)$$

uniquely determine all subsequent terms of S ; φ is called a *characteristic polynomial* of the *linear recurring sequence* S . It is well-known that these polynomials form a (*principal*) *ideal* Id_S of $\mathbb{F}[x]$, generated by a *minimal polynomial* of S .

The situation is similar for $n \geq 1$ and a finite sequence $s = s_0, \dots, s_{1-n}$ over \mathbb{F} i.e. $s_i \in \mathbb{F}$. If $\varphi \in \mathbb{F}[x]$, $1 \leq d = |\varphi| < n$ and

$$s_{i-d} = -(\varphi_{d-1} s_{i-d+1} + \dots + \varphi_0 s_i)/\varphi_d \quad \text{for } d+1-n \leq i \leq 0$$

then φ and s_0, \dots, s_{1-d} uniquely determine s_{-d}, \dots, s_{1-n} and φ is often called a '*characteristic polynomial*' of s . However, these do not form an ideal of $\mathbb{F}[x]$; the reader may easily find examples for which a sum of characteristic polynomials of s is not a characteristic polynomial.

2.3 Annihilating Polynomials and Solutions

Let $n \geq 1$ and $s = s_0, \dots, s_{1-n}$ be a finite sequence over D i.e. $s_i \in D$; s is *trivial* if $s = 0, \dots, 0 = 0^n$. The *generating function* of s is $\underline{s} = \sum_{i=1-n}^0 s_i x^i \in D[x^{-1}]$. We put $v = v(\underline{s})$ if s is understood, so that if s is non-trivial then $1 - n \leq v \leq 0$.

DEFINITION 2.1 ([11, Definition 2.7]) *Let $\varphi \in R$, $d = |\varphi|$ and $\varphi = \sum_{i=0}^d \varphi_i x^i$. If $n \geq 1$ and $s = s_0, \dots, s_{1-n}$ then φ is an annihilating polynomial of s , written $\varphi \in \text{Ann}(s)$, if*

$$(\varphi \cdot \underline{s})_i = \varphi_d s_{i-d} + \varphi_{d-1} s_{i-d+1} + \dots + \varphi_0 s_i = 0 \quad \text{for } d+1-n \leq i \leq 0. \quad (7)$$

We note that (7) is vacuously satisfied if $d = |\varphi| \geq n$, so that the previous definition is equivalent to [11, Definition 2.7] and

$$\{\varphi \in R^\times : |\varphi| \geq n\} \subseteq \text{Ann}(s)^\times = \{\varphi \in R^\times : (\varphi \cdot \underline{s})_i = 0 \text{ for } |\varphi| + 1 - n \leq i \leq 0\}.$$

We prefer 'annihilating polynomial' to 'characteristic polynomial' as we do not insist that $\text{lc}(\varphi)$ be a unit of D . Further, we may be unable to express s_{1-n} as a linear combination of s_0, \dots, s_{2-n} ; e.g. if $s = 0^{n-1}, 1$ then s_{1-n} is not a linear combination of 0's; if $D = \mathbb{Z}$ and $s = 2, 1$ we cannot express 1 as a multiple of 2 in D .

As in (5) we now have:

PROPOSITION 2.2 *For $n \geq 1$ and a sequence $s = s_0, \dots, s_{1-n}$ over D*

$$f_1 \in \text{Ann}(s)^\times \text{ if and only if } f_1 \in R^\times, v(f_1 \cdot \underline{s} - x f_2) \leq |f_1| - n \text{ and } x f_2 = [f_1 \cdot \underline{s}].$$

We say that $f = (f_1, f_2) \in R^\times \times R$ (or $x f_2 / f_1$ if f_1^{-1} exists) is a solution for s .

If $(\varphi, \psi) \in R^2$ is a solution for s and $d = |\varphi| \geq 0$ then $|\psi| = v + d - 1$. Also φ and s_0, \dots, s_{1-d} determine ψ , since for $1 \leq i \leq v + d$ we have $\psi_{i-1} = (x\psi)_i = [\varphi \cdot \underline{s}]_i = \sum_{j=0}^d \varphi_j s_{i-j}$ where $1-d \leq i-j \leq 0$. We include a proof of the following for completeness.

PROPOSITION 2.3 *Let (φ, ψ) be a solution for $s = s_0, \dots, s_{1-n}$. If $1 \leq d = |\varphi| < n$ and $\text{lc}(\varphi)$ is a unit of D then (i) $\varphi^{-1} \in D[[x^{-1}]]$; (ii) $\varphi, s_0, \dots, s_{1-d}$ determine s_{-d}, \dots, s_{1-n} .*

PROOF. If $\sigma = 1 - \varphi x^{-d} / \varphi_d \in D[x^{-1}]$ then $\varphi = \varphi_d x^d (1 - \sigma)$, $\sigma \neq 1$ since $\varphi \neq 0$ and

$$\frac{1}{\varphi} = \frac{1}{\varphi_d x^d (1 - \sigma)} = \varphi_d^{-1} x^{-d} (1 + \sigma + \sigma^2 + \dots) \in D[[x^{-1}]].$$

Thus $v(\underline{s} - x\psi/\varphi) = v(\varphi \cdot \underline{s} - x\psi) + v(1/\varphi) \leq |\varphi| - n - v(\varphi) = -n$, which implies that $(x\psi/\varphi)_i = s_i$ for $n-1 \leq i \leq 0$. We know that φ and s_0, \dots, s_{1-d} determine ψ . Hence φ and s_0, \dots, s_{1-d} determine s_{-d}, \dots, s_{1-n} . \square

Thus if f is a solution, $|f_1| < n$ and $\text{lc}(f_1)$ is a unit of D then s_0, \dots, s_{1-n} and f_1 define a linear recurring sequence S_f with $\underline{S}_f = x f_2 / f_1$ and $f_1 \in \text{Id}_{S_f}$.

2.4 First Examples and the Key Lemma 2.6

Our first examples include the inductive bases for various results below.

EXAMPLE 2.4 (i) The (finite) geometric sequence of length n with common multiple $m \in D^\times$ is given by $s_0 = 1$ and $s_i = m^{-i}$ for $1 - n \leq i \leq -1$. It will be convenient to allow $m = 0$ as well. Then $v = 0$ and $\underline{s} = m^{n-1}x^{1-n} + \dots + 1$. If $|x - m| + 1 - n = 2 - n \leq i \leq 0$ then $((x - m) \cdot \underline{s})_i = (x \cdot \underline{s})_i - (m \cdot \underline{s})_i = s_{i-1} - ms_i = 0$, so that $x - m \in \text{Ann}(s)^\times$. As $x - m$ is invertible, the corresponding solution is $x/(x - m)$.

(ii) Let $n \geq 2$, $a \in D^\times$ and $s = 0^{n-1}, a$. We have $\underline{s} = ax^{1-n}$, $x^n = x^{1-v} \in \text{Ann}(s)^\times$ and ax/x^n is a solution for s , but cannot express s_{1-n} as a linear combination of zeroes.

(iii) Let $D = \mathbb{Z}$ and $s = 2, 1$. We have the solution $(2x - 1, 2)$ but cannot express s_{-1} in terms of s_0 .

For $s = s_0, \dots, s_{1-n}$ and arbitrary $a \in D$, $t = s, a$ is the sequence s_0, \dots, s_{1-n}, a . Given a solution g for s we want to construct a solution h for t . We begin with first components. It is clear that $\text{Ann}(t)^\times \subseteq \text{Ann}(s)^\times$. Suppose that $g_1 \in \text{Ann}(s)^\times$. Then $g_1 \in \text{Ann}(t)$ if and only if $(g_1 \cdot \underline{t})_i = 0$ for $|g_1| - n \leq i \leq 0$. If $|g_1| + 1 - n \leq i \leq 0$ and $0 \leq j \leq |g_1|$ then $1 - n \leq i - j \leq 0$ and so $t_{i-j} = s_{i-j}$. Hence $(g_1 \cdot \underline{t})_i = (g_1 \cdot \underline{s})_i = 0$ for $|g_1| + 1 - n \leq i \leq 0$ and $g_1 \in \text{Ann}(t)$ if and only if $(g_1 \cdot \underline{t})_{|g_1|-n} = 0$.

DEFINITION 2.5 ([11, Definition 2.10], cf. [7]). Let $n \geq 1$, $s = s_0, \dots, s_{1-n}$ and $g_1 \in R^\times$. For arbitrary $a \in D$ and $t = s, a$ the discrepancy of g_1 and t is $\Delta(g_1; t) = (g_1 \cdot \underline{t})_{|g_1|-n}$.

In general, if $g_1 \in \text{Ann}(s)$ then $g_1 \cdot \underline{t} = G + \Delta(g_1; t)x^{|g_1|-n} + [g_1 \cdot \underline{t}]$ where $v(G) < |g_1| - n$. We recall the proof of the following lemma from [12] as it shows the usefulness of second components. Also, the polynomial $g_2 h_1 - g_1 h_2$ of the proof will reappear later.

LEMMA 2.6 ([12, Lemma 5.2], cf. [7, Theorem 1]) Let $n \geq 1$, $s = s_0, \dots, s_{1-n}$ and $g_1 \in \text{Ann}(s)^\times$. If $t = s, a$ and $g_1 \notin \text{Ann}(t)$ then for any $h_1 \in \text{Ann}(t)^\times$ we have $|h_1| \geq n+1-|g_1|$.

PROOF. Let $\Delta = \Delta(g_1; t) \neq 0$. We have $g_1 \cdot \underline{t} = G + \Delta x^{|g_1|-n} + x g_2$ where $v(G) < |g_1| - n$ and $x g_2 = [g_1 \cdot \underline{t}]$. Also $h_1 \cdot \underline{t} = H + x h_2$ where $v(H) < |h_1| - n$ and $x h_2 = [h_1 \cdot \underline{t}]$. Put $\varphi = g_2 h_1 - g_1 h_2 \in R$. Then

$$\begin{aligned} x \varphi &= (x g_2) h_1 - g_1 (x h_2) \\ &= (g_1 \cdot \underline{t} - G - \Delta x^{|g_1|-n}) h_1 - g_1 (h_1 \cdot \underline{t} - H) = -G h_1 + g_1 H - \Delta x^{|g_1|-n} h_1 \end{aligned}$$

where $v(-G h_1 + g_1 H) < |g_1| - n + |h_1|$ and $x \varphi \neq 0$ since D has no zero divisors. Hence $|g_1| + |h_1| - n = |x \varphi| \geq 1$. \square

For Example 2.4(i), if h is a solution for s then $|h_1| \geq 1$ since s is non-trivial. For Example 2.4(ii) with $n \geq 2$, $(1, 0)$ is a solution for $0, \dots, 0$ but not for s since $a \neq 0$, so if h is a solution for s then $|h_1| \geq -v + 1 = n$. This can also be proved directly, see [11, Proposition 3.5(c)].

2.5 Linear Complexity and Minimal Solutions

Next we discuss minimality. Firstly, $\text{Ann}(s)^\times \neq \emptyset$ since any polynomial of degree n annihilates s and the following definition makes sense.

DEFINITION 2.7 ([11, Definition 3.1]) *Let $n \geq 1$ and $s = s_0 \dots, s_{1-n}$. The linear complexity s is*

$$L_n = L(s) = \min\{|f_1| : f_1 \in \text{Ann}(s)^\times\}.$$

We say that f_1 is a minimal polynomial (MP) of s if $f_1 \in \text{Ann}(s)^\times$ and $|f_1| = L(s)$. We write $\text{MP}(s)$ for the set of minimal polynomials of s and say that $f \in \mathbb{R}^2$ is a minimal solution for s if it is a solution for s and $f_1 \in \text{MP}(s)$.

It is important to note that linear complexity and minimality are defined independently of how solutions are obtained. Of course, $0/1$ is a minimal solution for any sequence of zeroes, and $L(s) = 0$ if and only if s is trivial. For Example 2.4(ii), $x^n \in \text{Ann}(s)$, so $L_n = n$ by Lemma 2.6. The function L is a non-decreasing function of n and $L_n \leq n$. If $h_1 \in \text{Ann}(s, a)$ and $|h_1| = L(s)$ then $h_1 \in \text{MP}(s, a)$ since $L(s, a) \geq L(s) = |h_1| \geq L(s, a)$.

We repeat the proof of the next result from [11] for the convenience of the reader.

PROPOSITION 2.8 ([11, Corollary 3.24]) *Let $n \geq 1$, $s = s_0, \dots, s_{1-n}$ be a sequence over \mathbb{F} , f be a solution for s and $d = \gcd(f_1, f_2)$. Then (i) f/d is a solution for s ; (ii) if f is a minimal solution for s then $|f_1| \leq n$ and $d = 1$.*

PROOF. Let $f_1 \cdot \underline{s} = F + xf_2$ where $v(F) \leq |f_1| - n$ and $g = f/d$. Then $F/d \in \mathbb{F}[[x^{-1}]]$ and $g_1 \cdot \underline{s} = F/d + xg_2$ where $v(F/d) = v(F) - |d| \leq |f_1| - n - |d| = |g_1| - n$. Hence $g_1 \in \text{Ann}(s)$ and $[g_1 \cdot \underline{s}] = xg_2$ i.e. g is a solution for s . (ii) If f is a minimal solution then $|f_1| = L_n \leq n$ and $|f_1| = L_n \leq |g_1| = |f_1| - |d|$ and hence $|d| = 0$. \square

So if s is a sequence over \mathbb{F} , f is any minimal solution for s and $\underline{S}_f = xf_2/f_1$, $\text{Id}_{S_f} = f_1 \mathbb{F}[x]$ i.e. f_1 is a minimal polynomial for S_f . This justifies our use of the term 'minimal polynomial' of s . The converse of Proposition 2.8(ii) fails: let $n \geq 2$ and $s_i = m^{-i}$ for $1 - n \leq i \leq 0$ where $m \in \mathbb{F}^\times$; $x - m \in \text{MP}(s)$ and $L_n = 1$. Now $f_1 = x^n \in \text{Ann}(s)$, $f_2 = m^0 x^{n-1} + \dots + m^{n-1}$ and $\gcd(f_1, f_2) = 1$ since $m^{n-1} \neq 0$, but $f_1 \notin \text{MP}(s)$.

We will need to single out two kinds of non-trivial sequences:

DEFINITION 2.9 *Let $n \geq 1$ and $s = s_0, \dots, s_{1-n}$ be a sequence over D . We call s pseudo-geometric if $L_n = \dots = L_1 = 1$, and essential if $n \geq 2$ and $L_n > L_1 \geq 0$.*

Any geometric sequence s is pseudo-geometric since $x - s_{-1}/s_0 \in \text{MP}(s)$. A non-trivial sequence $s = a, 0^{n-1}$ is pseudo-geometric. In general, s is pseudo-geometric if and only if $s_0 x - s_{-1} \in \text{MP}(s)$. Conversely, if $n \geq 2$, s_0 is a unit of D and s is pseudo-geometric then s is a geometric sequence with common ratio s_{-1}/s_0 .

Essential sequences were motivated by the need for the integer

$$n' = \max_{1 \leq j < n} \{j : L_j < L_n\}$$

to be well-defined; now $s' = s_0, \dots, s_{1-n'}$ is a well-defined, proper subsequence of s as $1 \leq n' < n$.

N.B. For $n \geq 2$, the sequence $s = 0^{n-1}, a$ of Example 2.4(ii) is essential since $L_n = n > L_1 = 0$, $1 \leq n' = n - 1 < n$ (and moreover $s' = 0^{n-1}$ has minimal solution $0/1$). On the other hand, if s is pseudo-geometric then n' is undefined.

We can now formally state our subdivision of sequences.

PROPOSITION 2.10 *A sequence over D is either trivial, pseudo-geometric or essential.*

PROOF. We have $L_1 = \dots = L_n = 0$ if and only if s is trivial. Hence if s non-trivial, $L_i > 0$ for some i , $1 \leq i \leq n$. If $L_1 \neq 0$ then $L_1 = 1$ since $L_i \leq i$ for all i . If $1 = L_2 = \dots = L_n$ then s is pseudo-geometric; otherwise if i is the first integer with $L_i > 1$ then $L_n \geq L_i > 1$ i.e. s is essential. Finally, if $L_1 = 0$ then $L_i \neq 0$ for some i , $2 \leq i \leq n$ as s is non-trivial, so $L_n \geq L_i > L_1 = 0$ and s is essential. \square

PROPOSITION 2.11 *If $n \geq 2$, $s = s_0, \dots, s_{1-n}$ is pseudo-geometric and $\mu_1 \in \text{MP}(s)$ satisfies $\Delta(\mu_1; s, s_{-n}) \neq 0$ then s, s_{-n} is essential.*

PROOF. By Lemma 2.6, $L_{n+1} \geq n + 1 - L_n = n \geq 2 > 1 = L_1$. \square

The first state diagram of the Introduction illustrates this transition on adding a term.

3 Minimal Solutions via Partial Quotients

Here we revisit the first part of [9, Theorem 1]. Let S be an infinite sequence over \mathbb{F} , \underline{S} its generating function and $n \geq 1$. Our goal is to show that a certain partial quotient of \underline{S} (depending on n) is a minimal solution for $S|n = S_0, \dots, S_{1-n}$. In particular, we relate $L(S|n)$ to the degrees of the partial quotients of \underline{S} .

We recall the construction of the partial quotients of \underline{S} , their basic identities and properties. We work through [15, Example 1]. Then we discuss geometric sequences and $0^{n-1}, S_{1-n}$, where $S_{1-n} \in \mathbb{F}^\times$ and $n \geq 2$. These form our inductive basis for the main Theorem 3.7. When $S|n$ is essential, we determine $\max_{1 \leq j < n} \{L_j < L_n\}$ and prove an identity for any $f \in \mathbb{R}^2$.

3.1 Continued Fractions

We use the formulation of continued fractions in $\mathbb{F}[[x^{-1}]]$ from [9]; in particular, we also use $\text{Pol}(L) = \sum_{i=0}^{v(L)} L_i x^i \in \mathbb{R}$ for $L \in \mathbb{F}((x^{-1}))$. It is well known that \underline{S} has the unique continued fraction expansion $0 + x/(a_1 + 1/(a_2 + \dots)) = [0, a_1, a_2, \dots]$ where, if $a_i \in \mathbb{R}$ exists, then $|a_i| \geq 1$. The a_i are obtained using division in the field $\mathbb{F}((x^{-1}))$ as follows:

$a_0 \leftarrow 0; b_0 \leftarrow x^{-1}\underline{S}; q^{(-1)} \leftarrow (0, 1); q^{(0)} \leftarrow (1, 0);$

$i \leftarrow 0;$

while ($b_i \neq 0$)

$\lceil a_{i+1} \leftarrow \text{Pol}(b_i^{-1}); q^{(i+1)} \leftarrow a_{i+1}q^{(i)} + q^{(i-1)};$

$b_{i+1} \leftarrow b_i^{-1} - a_{i+1}; i \leftarrow i + 1; \rfloor$

The *partial quotients* of \underline{S} are $\{q^{(i)} \in \mathbb{R}^2 : i \geq 0\}$. Put $|q_1^{(-1)}| = 0$ and if $b_i = 0$ (i.e. a_{i+1} and $q^{(i+1)}$ do not exist) put $|a_{i+1}| = |q_1^{(i+1)}| = \infty$. In the following well-known result, Part (iv) on numerators is probably well-known, but does not appear in [9].

THEOREM 3.1 *If $i \geq 1$, $q = q^{(i)}$ exists and $q' = q^{(i-1)}$ then $|q_1| = \sum_{j=1}^i |a_j| \geq 1$. In particular, if $i \geq 0$ then $1 - |q_1^{(i+1)}| \leq 0$.*

If $i \geq 0$ and q exists then

(i) $q_2 q'_1 - q_1 q'_2 = (-1)^{i-1}$ and $\gcd(q_1, q'_1) = \gcd(q_2, q'_2) = 1$;

(ii)

$$\underline{S} = \frac{x(q_2 + b_i q'_2)}{q_1 + b_i q'_1};$$

(iii) $v(q_1 \cdot \underline{S} - x q_2) = 1 - |q_1^{(i+1)}|$ so that $\text{Pol}(q_1 \cdot \underline{S} - x q_2) = 0$;

(iv) $|a_1| = 1 - v$, $|q_2| = \sum_{j=2}^i |a_j| = |q_1| - |a_1|$ if $i \geq 1$ and $\text{Pol}(q_1 \cdot \underline{S}) = [q_1 \cdot \underline{S}] = x q_2$.

If $i \geq 1$ is the first index for which $b_i = 0$ then

(v) $\underline{S} = x q_2 / q_1$ and $v(q_1 \cdot \underline{S} - x q_2) = -\infty = 1 - |q_1^{(i+1)}|$;

(vi) $\text{Pol}(q_1 \cdot \underline{S}) = x q_2$ and $|q_2| = v + |q_1| - 1 < |q_1|$.

PROOF. (i)-(iii) Use induction and properties of the exponential valuation as in [9]. (iv) For $i \geq 1$, $|q_2| = \sum_{j=2}^i |a_j|$ is an easy induction. We have $|a_1| = |\text{Pol}(x/\underline{S})| = 1 - v$ so that $|q_2| = |q_1| - |a_1| = |q_1| + v - 1$ and

$$\text{Pol}(q_1 \cdot \underline{S}) = \text{Pol}(q_1 \cdot \underline{S} - x q_2) + \sum_{j=0}^{v+|q_1|} (x q_2)_j x^j = x \sum_{k=-1}^{|q_2|} (q_2)_k x^k = x q_2$$

by (iii). (v) If $i \geq 1$, $b_{i-1} \neq 0$ and $b_i = 0$ then

$$q = q + (b_{i-1}^{-1} - a_i)q' = q - a_i q' + b_{i-1}^{-1} q' = q^{(i-2)} + b_{i-1}^{-1} q'$$

and rearranging gives

$$\frac{x q_2}{q_1} = \frac{x(q'_2 + b_{i-1} q_2^{(i-2)})}{q'_1 + b_{i-1} q_1^{(i-2)}} = \underline{S}$$

by (ii). (vi) Immediate. □

Next we define a partition of \mathbb{N}^\times . Let $n_0 = 1$ and for $i \geq 1$, define $n_i = n_i(S)$ by

$$n_i = |q_1^{(i-1)}| + |q_1^{(i)}|.$$

From Theorem 3.1 we have $1 = n_0 \leq n_1 < n_2 < \dots$ and $\{[n_i, n_{i+1}) : i \geq 0\}$ is a partition of \mathbb{N}^\times (except that $[n_0, n_1) = \emptyset$ if $n_1 = 1$) for if $i \in \mathbb{N}$ is largest such that $n_i \leq n$ then $n \in [n_i, n_{i+1})$ and i is clearly unique. Thus if $\underline{S} = 0$, $n_1 = \infty$ and for all $n \geq 1$, $0/1$ is a minimal solution for $S|n$.

The next example is [15, Example, p. 21]. Here $\mathbb{F} = \mathbb{F}_2[x]/(x^4 + x + 1)$ and α generates \mathbb{F}^\times . For the table of \mathbb{F}^\times as polynomials in α , see [6, p. 85].

EXAMPLE 3.2 Let $\underline{S} = x(\alpha^5 x^2 + \alpha^2 x + \alpha^{10})/(x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{13}) \in \mathbb{F}(x)$. Direct calculation gives

i	b_i	a_{i+1}	$b_{i+1} = b_i^{-1} - a_{i+1}$
0	$x^{-1}\underline{S}$	$\alpha^{10}x + \alpha^{14}$	$(\alpha^6 x + \alpha^{10})/(\alpha^5 x^2 + \alpha^2 x + \alpha^{10})$
1	$(\alpha^6 x + \alpha^{10})/(\alpha^5 x^2 + \alpha^2 x + \alpha^{10})$	$\alpha^{14}x + \alpha^5$	$\alpha^5/(\alpha^6 x + \alpha^{10})$
2	$\alpha^5/(\alpha^6 x + \alpha^{10})$	$\alpha x + \alpha^5$	0

i	$q^{(i-1)}$	$q^{(i)}$	$q^{(i+1)} = a_{i+1} q^{(i)} + q^{(i-1)}$
0	(0, 1)	(1, 0)	$(\alpha^{10}x + \alpha^{14}, 1)$
1	(1, 0)	$(\alpha^{10}x + \alpha^{14}, 1)$	$(\alpha^9 x^2 + \alpha^6 x + \alpha, \alpha^{14}x + \alpha^5)$

and $q^{(3)}$ is

$$(\alpha^{10}x^3 + \alpha^{13}x^2 + \alpha^3x + \alpha^8, x^2 + \alpha^{12}x + \alpha^5) = \alpha^{10}(x^3 + \alpha^6x^2 + \alpha^3x + \alpha^{13}, \alpha^5x^2 + \alpha^2x + \alpha^{10}).$$

Clearing denominators, this is the extended Euclidean algorithm: a_{i+1} is the quotient and b_{i+1} is the remainder. We have $|q_1^{(0)}| = 0$, $|q_1^{(1)}| = 1$, $|q_1^{(2)}| = 2$ and $|q_1^{(3)}| = 3$ and $|q_1^{(4)}| = \infty$, so that the partition of \mathbb{N}^\times defined by S is $[1, 3), [3, 5), [5, \infty)$.

Our inductive proof of the first part of [9, Theorem 1] depends on characterising solutions for $S|n$ in terms of solutions for S , and is proved using Proposition 2.2.

LEMMA 3.3 Let $D = \mathbb{F}$ be a field. If $f_1 \in R^\times$, $|f_1| \leq n$ and $s = S|n$ then $[f_1 \cdot \underline{S}] = [f_1 \cdot \underline{s}] = x f_2$ say. Further f is a solution for s if and only if $v(f_1 \cdot \underline{S} - x f_2) \leq |f_1| - n$.

PROOF. We have $v(\underline{S} - \underline{s}) \leq -n$ and $[f_1 \cdot (\underline{S} - \underline{s})] = 0$, so $[f_1 \cdot \underline{S}] = [f_1 \cdot (\underline{s} + (\underline{S} - \underline{s}))] = [f_1 \cdot \underline{s}] + [f_1 \cdot (\underline{S} - \underline{s})] = [f_1 \cdot \underline{s}]$ and

$$f_1 \cdot \underline{S} - x[f_1 \cdot \underline{S}] = f_1 \cdot (\underline{s} + (\underline{S} - \underline{s})) - x[f_1 \cdot \underline{s}] = f_1 \cdot \underline{s} - x[f_1 \cdot \underline{s}] + f_1 \cdot (\underline{S} - \underline{s}).$$

Hence $v(f_1 \cdot \underline{S} - x[f_1 \cdot \underline{S}]) \leq \max\{v(f_1 \cdot \underline{s} - x[f_1 \cdot \underline{s}]), |f_1| - n\}$ and if $f_1 \in \text{Ann}(s)$ then $v(f_1 \cdot \underline{S} - [f_1 \cdot \underline{S}]) \leq |f_1| - n$ by Proposition 2.2. The converse is proved similarly, for $f_1 \cdot \underline{s} - x[f_1 \cdot \underline{s}] = f_1 \cdot \underline{S} - x[f_1 \cdot \underline{S}] - f_1 \cdot (\underline{S} - \underline{s})$. \square

3.2 Geometric Sequences

If $S_0 \neq 0$, Theorem 3.1 implies that $n_1 = |a_1| = 1 - v = 1$.

PROPOSITION 3.4 *Let S be an infinite sequence over a field \mathbb{F} such that $S_0 \neq 0$, $q = q^{(1)}$ and $q' = (1, 0)$. The following are equivalent*

- (i) $n \in [n_1, n_2]$;
- (ii) q' is not a solution for $s = S|n$ and q is a minimal solution for s .

PROOF. (i) \Rightarrow (ii). Firstly q' is not a solution for s since $S_0 \neq 0$. Secondly, $|q_1| \leq n$ and

$$v(q_1 \cdot \underline{S} - x q_2) = 1 - |q_1^{(2)}| = 1 - (n_2 - 1) = 2 - n_2 \leq 1 - n.$$

By Lemma 3.3, q is a solution for s . As $|q_1| = 1$, it is a minimal solution.

(ii) \Rightarrow (i). If $n \notin [n_1, n_2]$ then $n \in [n_2, n_3]$ so $v(q_1 \cdot \underline{S} - x q_2) = 1 - |q_1^{(2)}| = 2 - n_2 > 1 - n$ and $q_1 \notin \text{Ann}(s)$. In particular, $q_1 \notin \text{MP}(s)$. \square

We can say more.

PROPOSITION 3.5 *Let $S_0 \neq 0$ and $r = S_{-1}/S_0$. Then $a_1 = (x - r)/S_0$ and $n_2 \geq 3$.*

PROOF. Write $\underline{T} = \underline{S}/S_0 = 1 + rx^{-1} + \dots$; if this is a geometric series then $\underline{T} = x/(x - r)$, $b_0 = x^{-1}\underline{S} = S_0/(x - r)$, $a_1 = \text{Pol}(b_0^{-1}) = (x - r)/S_0$ and $n_2 = \infty$.

Otherwise we have $\underline{T} = 1 + rx^{-1} + r^2x^{-2} + \dots + r^{n_2-2}x^{2-n_2} + T_{1-n_2} + \dots$ where $T_{1-n_2} \neq rT_{2-n_2}$ and $2 - n_2 \leq -1$. Now $\underline{T} = x/(x - r) + \underline{U}$ for some \underline{U} with $v(\underline{U}) \leq 1 - n_2 \leq -2$ and

$$b_0/S_0 = x^{-1}\underline{S}/S_0 = x^{-1}\underline{T} = (x - r)^{-1} + x^{-1}\underline{U} = \frac{1 + (x - r)x^{-1}\underline{U}}{x - r} = \frac{1 - \underline{V}}{x - r}$$

say, where $v(\underline{V}) \leq -2$. Thus for all $i \geq 1$ we have $v(\underline{V}^i) \leq -2i \leq -2$,

$$b_0^{-1} = S_0^{-1}(x - r)/(1 - \underline{V}) = S_0^{-1}(x - r)(1 + \underline{V} + \underline{V}^2 + \dots)$$

and $a_1 = \text{Pol}(b_0^{-1}) = (x - r)/S_0$. \square

3.3 Essential Sequences and the General Case

If $S_0 = 0$, Theorem 3.1 implies that $n_1 = |a_1| = 1 - v > 1$.

PROPOSITION 3.6 *Let S be an infinite sequence over a field \mathbb{F} such that $\underline{S} \neq 0$, $S_0 = 0$, $q = q^{(1)}$ and $q' = (1, 0)$. The following are equivalent*

- (i) $n \in [n_1, n_2]$;
- (ii) q' is not a solution for $s = S|n$ and q is a minimal solution for s .

PROOF. (i) \Rightarrow (ii). Let $n \in [n_1, n_2)$. We have $|q_1| = 1 - v = n_1 \leq n$ and

$$v(q_1 \cdot \underline{S} - x q_2) = 1 - |q_1^{(2)}| = 1 + |q_1| - n_2 \leq |q_1| - n$$

from Theorem 3.1, so that q is a solution for s by Lemma 3.3. As $n_1 - 1 \geq 1$ and $1 \in \text{Ann}(S|_{n_1-1}) \setminus \text{Ann}(S|_{n_1})$, Lemma 2.6 implies that $1 - v = |q_1| \geq L_n \geq L_{n_1} \geq n_1 - L_{n_1-1} = n_1 = 1 - v$ so $L_n = 1 - v$ and q is a minimal solution for s .

(ii) \Rightarrow (i). If $n \notin [n_1, n_2)$ then either (a) $n \in [1, n_1)$, $v(q'_1 \cdot \underline{S} - x q'_2) = 1 - |q_1| = 1 - n_1 \leq -n$ and $q'_1 = 1 \in \text{Ann}(s)$ or (b) $n \in [n_2, n_3)$ and as in the proof of Proposition 3.4, $v(q_1 \cdot \underline{S} - x q_2) = 1 - |q_1^{(2)}| = 2 - n_2 > 1 - n$, so $q_1 \notin \text{Ann}(s)$ and $q_1 \notin \text{MP}(s)$. \square

We have now treated the case $n \in [n_1, n_2)$. Now for the general case.

THEOREM 3.7 (Cf. [9, Theorem 1], [2, Theorem 4]) *Let $\underline{S} \neq 0$, $i \geq 1$ and $q = q^{(i)}$, $q' = q^{(i-1)}$. The following are equivalent:*

- (i) $n \in [n_i, n_{i+1})$;
- (ii) q' is not a solution for $s = S|_n$ and q is a minimal solution for s .

PROOF. For $i = 1$ the result follows from Propositions 3.4 and 3.6. Suppose inductively that $i \geq 2$ and that the result is true for $i - 1$.

(i) \Rightarrow (ii). Let $n \in [n_i, n_{i+1})$. Then $0 \leq |q'_1| = n_i - |q_1| \leq n - |q_1|$ i.e. $|q_1| \leq n$ and Lemma 3.3 applies. If $n < n_{i+1}$ then by Theorem 3.1

$$v(q_1 \cdot \underline{S} - x q_2) = 1 - |q_1^{(i+1)}| = 1 - n_{i+1} + |q_1| \leq |q_1| - n$$

so $q_1 \in \text{Ann}(s)$. Likewise $|q'_1| < |q_1| \leq n$ and Lemma 3.3 applies to q'_1 : if $n_i \leq n$ then

$$v(q'_1 \cdot \underline{S} - x q'_2) = 1 - |q_1| = 1 - n_i + |q'_1| \geq 1 + |q'_1| - n$$

i.e. $q'_1 \notin \text{Ann}(s)$. We next show that $q_1 \in \text{MP}(S|_{n_i})$. Since $q_1 \in \text{Ann}(s)$ we have $q_1 \in \text{Ann}(S|_{n_i})$, so $|q_1| \geq L_{n_i}$. We have $n_i \geq n_2 > n_1 \geq 1$ i.e. $n_i - 1 \geq 1$. The inductive hypothesis and Lemma 3.3 imply that $q'_1 \in \text{Ann}(S|_{n_i-1}) \setminus \text{Ann}(S|_{n_i})$. So Lemma 2.6 implies that $|q_1| \geq L_{n_i} \geq n_i - |q'_1| = |q_1|$ and hence $|q_1| = L_{n_i}$. Now let $n_i + 1 \leq n < n_{i+1}$. We know that $q_1 \in \text{Ann}(s)$, so $L_n \leq |q_1| = L_{n_i}$. But $n \geq n_i$ implies that $L_n \geq L_{n_i}$, so $L_n = L_{n_i}$ and $q_1 \in \text{MP}(s)$.

(ii) \Rightarrow (i). If $n \notin [n_i, n_{i+1})$ either (a) $n \in [n_{i-1}, n_i)$ and $q'_1 \in \text{Ann}(s)$ or (b) $n \in [n_{i+1}, n_{i+2})$ and so $q_1 \notin \text{Ann}(s)$ by the first part, and in particular $q_1 \notin \text{MP}(s)$. \square

It follows that for Example 3.2, we have $L_1 = L_2 = 1$, $L_3 = L_4 = 2$ and $L_5 = L_6 = 3$. We list some simple consequences of Theorem 3.7:

PROPOSITION 3.8 *Let $n \geq 1$, $s = S|_n$ be non-trivial. Then*

- (i) *either s is geometric or essential;*
- (ii) $L_{n_i} = \sum_{k=1}^i |a_k|$ *and we can obtain L_{n_i} without computing partial quotients;*
- (iii) *if $n_{i+1} < \infty$ then on the interval $[n_i, n_{i+1})$, $L_{n_i} = |q_1^{(i)}|$ appears $n_{i+1} - n_i$ times.*

PROOF. We prove (i) only. As s is non-trivial, $n \notin [1, n_1)$ i.e. $n \in [n_i, n_{i+1})$ for some $i \geq 1$ and $n_1 = |q_1| = |a_1| = 1 - v$. If $i \geq 2$ then $L_n = L_{n_i} \geq L_{n_2} > L_{n_1} \geq L_1$ i.e. s is essential. Now suppose that $i = 1$ i.e. $n \in [n_1, n_2)$. If $v = 0$ then $|q_1| = 1$, $L_n = L_{n_1} = L_1 = 1$ and s is geometric. If $v < 0$, $n_1 = |q_1| > 1$ and $L_n = L_{n_i} \geq L_{n_1} = 1 - v \geq 2$ and $L_{n_1} > L_1 = 0$ i.e. s is essential. \square

We note that in the previous proposition, if $n \in [n_1, n_2)$ and $b_1 = 0$ (i.e. $n_2 = \infty$) then $S|n$ is geometric; otherwise for $k \in [n_i, n_{i+1})$ and $i \geq 2$, $S|k$ will be essential. The second state diagram of the Introduction illustrates this behaviour.

COROLLARY 3.9 (Cf. [7, Theorem 1]) *Let $n \geq 1$ and $s = S|n$ be non-trivial. Then*

- (i) *either $L_{n+1} = L_n$ or $L_{n+1} = n + 1 - L_n > L_n$;*
- (ii) *if $n \in [n_i, n_{i+1})$ and $q_1^{(i)} \notin \text{Ann}(S|n + 1)$ then $L_{n+1} = \max\{L_n, n + 1 - L_n\}$.*

PROOF. We know that $n \in [n_i, n_{i+1})$ for some $i \geq 1$. (i) From Theorem 3.7, if $n + 1 \in [n_i, n_{i+1})$ then $L_{n+1} = L_{n_i} = L_n$. Otherwise $n + 1 = n_{i+1} = L_{n_i} + L_{n_{i+1}} = L_n + L_{n+1}$ and $L_{n+1} = L_{n_{i+1}} > L_{n_i} = L_n$. (ii) If $L_n \geq n + 1 - L_n$ then $L_{n+1} = L_n$ by Part (i). Suppose now that $L_n < n + 1 - L_n$. Since $n + 1 - L_n \leq L_{n+1}$ by Lemma 2.6, $L_n < L_{n+1}$ and by Part (i) we have $L_{n+1} = n + 1 - L_n$. We conclude that $L_{n+1} = \max\{L_n, n + 1 - L_n\}$. \square

If $S|n$ is essential, the integer $\max_{1 \leq j < n} \{j : L_j < L_n\}$ equals $n_i - 1$:

COROLLARY 3.10 *If $L_n > L_1 \geq 0$, $n \in [n_i, n_{i+1})$, $s = S|n$, $q = q^{(i)}$, $q' = q^{(i-1)}$ and $n' = n_i - 1$ then*

- (i) *q' is a minimal solution for $s' = S|n'$;*
- (ii) *$n' = \max_{1 \leq j < n} \{j : L_j < L_n\}$ and $L_n + L_{n'} = n' + 1$;*
- (iii) *$[q_1 \cdot \underline{s}] = xq_2$ and $[q'_1 \cdot \underline{s}] = xq'_2$.*

PROOF. We know that $n \in [n_i, n_{i+1})$ for some $i \geq 1$ and $L_{n_i} = L_n > L_1 \geq 0$. Hence $n' \geq 1$ and s' is well-defined. As $n' \in [n_{i-1}, n_i)$, $q'_1 \in \text{MP}(s')$ by Theorem 3.7. (ii) We have $L_{n'} = L_{n_{i-1}} < L_{n_i} = L_n$ and so $n' = \max_{1 \leq j < n} \{j : L_j < L_n\}$. Also $L_n + L_{n'} = |q| + |q'| = n_i = n' + 1$. (iii) We have $[q_1 \cdot \underline{s}] = [q_1 \cdot \underline{S}] = xq_2$ by Lemma 3.3 since $|q_1| = L_{n_i} \leq n_i \leq n$. Likewise $|q'_1| < |q_1| \leq n$ and $[q'_1 \cdot \underline{s}] = [q'_1 \cdot \underline{S}] = xq'_2$. \square

We conclude with a consequence of Theorem 3.1 and Corollary 3.10.

PROPOSITION 3.11 *Suppose that $L_n > L_1 \geq 0$, $n \in [n_i, n_{i+1})$, $q = q^{(i)}$ and $q' = q^{(i-1)}$. If $f \in \mathbb{R}^2$, $m = f_2 q_1 - f_1 q_2$ and $m' = f_2 q'_1 - f_1 q'_2$ then*

$$(-1)^{i-1} f_1 = m' q_1 - m q'_1.$$

PROOF. As q' is well-defined from Corollary 3.10, we have $m' q_1 - m q'_1 = (f_2 q'_1 - f_1 q'_2) q_1 - (f_2 q_1 - f_1 q_2) q'_1 = f_1(q_2 q'_1 - q_2' q_1)$, which is $(-1)^{i-1} f_1$ by Theorem 3.1. \square

4 An Inductive Construction of Minimal Solutions

In this section, we work with arbitrary finite sequences over D . Given $n \geq 1$, we construct a minimal solution μ for any $s = s_0, \dots, s_{1-n}$ i.e. $\mu_1 \in \text{Ann}(s)$ and $|\mu_1| = L_n = L$ say. If $L < n$ and $\text{lc}(\mu_1)$ is a unit of D , we can 'generate' s_{-L}, \dots, s_{1-n} using s_0, \dots, s_{1-L} and μ_1 . For Examples 2.4(ii), (iii) we will see that the construction returns $\mu_1 = x^n$ and $\mu_1 = 2x - 1$ respectively; in each case, we cannot generate s_{1-n} using s_0, \dots, s_{2-n} and μ_1 .

We simplify [11] by appealing to Proposition 2.10 and recalling two lemmas from [11]. In this way we construct a new minimal solution when the current one fails. The proof of each lemma consists of (i) verifying that we have a new solution and (ii) applying Lemma 2.6 to deduce minimality. For a pseudo-geometric sequence, it suffices to consider $n + 1 - 2L = n - 1 > 0$ only and the proof is elementary. However, for an essential sequence, we require both a current minimal solution and a solution for $s_0, \dots, s_{1-n'}$ where $1 \leq n' < n$. We encode each of these solutions as a 'triple'.

The resulting Algorithm 4.12 is identical to [11, Algorithm 4.6], except that we compute μ_2 rather than $x\mu_2$. We can also suppress second components and in this way compute minimal polynomials only, cf. [7]. We include a normalised version to compute a monic μ_1 when D is a field. We also give a new analysis of Algorithm 4.12.

Section 4.5 defines the scalar $\nabla_s \in D^\times$ and proves Identities (2), (3) of the Introduction, see Propositions 4.20, 4.22. These identities are integral to the rest of the paper.

4.1 Pseudo-Geometric Sequences

The following integer will play an important role for all finite sequences.

DEFINITION 4.1 For $n \geq 1$ and $s = s_0, \dots, s_{1-n}$ we put $e_s = n + 1 - 2L_n \in \mathbb{Z}$.

LEMMA 4.2 ([11, Theorems 3.8, 4.5]) Let $k \geq 1$, $r = s_0, \dots, s_{1-k}$, $s_0 \neq 0$ and μ be a minimal solution for r with $L_k = |\mu_1| = 1$. If $s = r, s_{-k}$ and $\Delta_1 = \Delta(\mu_1; s) \neq 0$ then $\nu = s_0 x^{e_r} \mu - \Delta_1(1, 0)$ is a minimal solution for s ; in fact $|\nu_1| = \max\{1, 1 + e_r\}$.

We apply this as follows. If $n = 1$ and $s_0 \neq 0$ then $\mu = (x, s_0)$, a pseudo-geometric sequence and $e_{s_0} = 0$. For $n = 2$, $r = s_0$ and $s = r, s_{-1}$, if $\Delta_1 = s_{-1} \neq 0$ then $\nu = s_0 x^0(x, s_0) - s_{-1}(1, 0) = (s_0 x - s_{-1}, s_0^2)$ since $e_r = 0$; s is also pseudo-geometric. Let $n \geq 3$ and $s = r, s_{1-n}$. If $L_{n-1} = \dots = L_1$, μ is a minimal solution for r and $\Delta_1 = \Delta(\mu_1; s) \neq 0$, then $\nu = s_0 x^{n-2} \mu - \Delta_1(1, 0)$ since $e_r = n - 2$. Now $L_n = |\nu_1| = n - 1 > L_1 = 1$; the new sequence s is essential. This is an explicit version of Proposition 2.11.

EXAMPLES 4.3 Let $a, b \in D^\times$. (i) Put $r = a$ and $s = r, b$. We begin with $\mu = (x, a)$ and $\Delta_1 = \Delta(\mu; s) = b \neq 0$. Lemma 4.2 shows that $a(x, a) - b(1, 0) = (ax - b, a^2)$ is a minimal solution for s . If a is a unit of D and $m = b/a$, we have $s = a, ma$ i.e. Example 2.4(i) and since $ax - b \in \text{MP}(s)$, we have $x - m \in \text{MP}(s)$.

(ii) Now let $k = 2$, $r = a, b$ and $s = r, c$. We know that $(ax - b, a^2)$ is a minimal solution for r and

$$\Delta_1 = \Delta(ax - b; s) = ((ax - b) \cdot (cx^{-2} + bx^{-1} + a))_{1-2} = ac - b^2.$$

Lemma 4.2 implies that if $\Delta_1 \neq 0$, $ax(ax - b, a^2) - \Delta_1(1, 0) = (a^2x^2 - abx - \Delta_1, a^3x)$ is a minimal solution for s . Taking $D = \mathbb{Z}$, $a = b = 1$ and $c = 2$, we see that $x^2 - x - 1 \in \text{MP}(1, 1, 2)$, as expected. Further, if $f_1 = x^3$ then $f_2 = x^2 + x + 2$ and $\gcd(f_1, f_2) = 1$. Thus the converse of Proposition 2.8 fails for essential sequences too.

(iii) Let the common multiple m in Example 2.4(i) be zero, so that $r = a, 0^{k-1}$ where $k \geq 2$ and $\mu = (x, a)$ i.e. $e_r = k - 1$. If $s = r, b$ where $b \in D^\times$ then $\Delta_1 = \Delta(x; s) = b \neq 0$, hence $ax^{k-1}(x, a) - b(1, 0) = (ax^k - b, a^2x^{k-1})$ is a minimal solution for s and $L_{k+1} = k > 1 = L_k$.

4.2 Essential Sequences or, a Tale of Two Triples

Next we recall a lemma which constructs a minimal solution for an essential sequence when the current one fails. As this is more involved, we encode the data as a 'triple' consisting of a strictly positive integer, a minimal polynomial and an element of D^\times . We also require that our two triples are linked by linear complexity. Thus given a pair of linked triples for r and $a \in D$, we construct a pair of linked triples for $s = r, a$.

DEFINITION 4.4 Let $k \geq 1$, $r = s_0, \dots, s_{1-k}$ be essential and $s_{-k} \in D$. A linked pair of triples (for r) consists of $T_r = (k, \mu_1, \Delta_1)$, $T'_r = (k', \mu'_1, \Delta'_1) \in \mathbb{N}^\times \times R \times D^\times$ such that

- (i) $s = r, s_{-k}$, $\Delta_1 = \Delta(\mu_1; s)$, $\mu_1 \in \text{MP}(r) \setminus \text{Ann}(s)$;
- (ii) $k' = \max_{1 \leq j < k} \{j : L_j < L_k\} < k$ so that $r' = s_0, \dots, s_{1-k'}$ is a well-defined, proper subsequence of r ;
- (iii) $s' = r', s_{-k'}$, $\Delta'_1 = \Delta(\mu'_1; s')$, $\mu'_1 \in \text{MP}(r') \setminus \text{Ann}(s')$ and $L_k + L_{k'} = k' + 1$.

EXAMPLE 4.5 Let $a, b \in D^\times$.

(i) Let $r = a, 0^{k-1}$ with $k \geq 2$ (a pseudo-geometric sequence with common multiple 0), $s = r, b$ and $\nu = (ax^k - b, a^2x^{k-1})$ be a minimal solution for s as in Example 4.3(iii). Let $T'_s = (k, x, b)$ and suppose that $\Delta_1 = \Delta(\nu_1; s, c) \neq 0$ for some $c \in D$. Then $T_s = (k + 1, \nu_1, \Delta_1)$ and T'_s are linked: for $i \leq k$ we have $L_i = 1$, so $(k + 1)' = k$ and $L_{k+1} + L_{(k+1)'} = k + 1 = (k + 1)' + 1$.

(ii) Let $k \geq 2$ and $r = 0^{k-1}, a$ where $k \geq 2$, so $v = 1 - k$. We claim that $T_r = (k, x^k, b)$ and $T'_r = (k - 1, 1, a)$ are linked. We have $\Delta(1; 0^{k-1}) = a \neq 0$, giving the triple $T'_r = (-v, 1, a)$ i.e. $k' = -v = k - 1$ and $L_{k'} = 0$. We also know that (x^k, a) is a minimal solution for r . Let $s = r, b$ where $b \neq 0$. Then

$$\Delta(x^k; s) = (x^k \cdot \underline{s})_{k-k} = s_{-k} = b \neq 0.$$

giving the triple $T_r = (k, x^k, b)$. Furthermore T_r, T'_r are linked since $L_k + L_{k'} = k = k' + 1$.

REMARK 4.6 In [11], we used $T_r = (1, x, \Delta_1)$, $T'_r = (0, 1, s_0)$, linked by $L_0 = 0$ when $r = s_0 \neq 0$. In this paper, we treat pseudo-geometric sequences separately and the proper subsequence r' always has length $n' \geq 1$, further simplifying the theory developed in [11].

We now combine several results from [11] to construct a linked triple for $s = r, s_{-k}$ from a linked triple for r .

LEMMA 4.7 ([11, Proposition 3.11, Theorem 3.13, Proposition 4.4]) Let $k \geq 2$, $r = s_0, \dots, s_{1-k}$ be essential and $s = r, s_{-k}$. Suppose that $T_r = (k, \mu_1, \Delta_1)$, $T'_r = (k', \mu'_1, \Delta'_1)$ are linked triples for r . If

$$\nu = \begin{cases} \Delta'_1 \mu - \Delta_1 x^{-e} \mu' & \text{if } e = e_r \leq 0 \\ \Delta'_1 x^{+e} \mu - \Delta_1 \mu' & \text{otherwise} \end{cases}$$

then $|\nu_1| = \max\{L_k, L_k + e_r\} = \max\{L_k, k + 1 - L_k\}$, $\nu_1 \in \text{MP}(s)$ and $x\nu_2 = [\nu_1 \cdot t]$ i.e. ν is a minimal solution for s . Further, if

(a) $\Delta = \Delta(\nu_1; s, s_{-k-1}) \neq 0$ and $T_s = (k + 1, \nu_1, \Delta)$;

(b) $T'_s = T'_r$ if $e_r \leq 0$ and $T'_s = (k, \mu_1, \Delta_1)$ if $e_r \geq 1$;

then T_s, T'_s are linked. Finally $e_s = 1 + e_r$ if $e_r \leq 0$, and $e_s = 1 - e_r$ otherwise.

PROOF. We show only that T_s, T'_s are linked. (The remaining item on updating e_s is a simple verification.) Let $m_k = \max_{1 \leq j < k} \{j : L_j < L_k\}$ and $\mu_1 \in \text{MP}(r)$. If $e_r \leq 0$ then $L_{k+1} + L_{(k+1)'} = L_k + L_{k'} = k' + 1 = (k + 1)' + 1$ and $(k + 1)' = k' = m_k = m_{k+1}$. Otherwise $L_{k+1} + L_{(k+1)'} = (k + 1 - L_k) + L_k = k + 1 = (k + 1)' + 1$ and $(k + 1)' = k = m_{k+1}$ since $L_k < k + 1 - L_k = L_{k+1}$. \square

EXAMPLE 4.8 (i) For Example 4.5(ii), Theorem 4.7 yields $\nu_1 = ax^k - bx^{k-1}$ from $T_r = (k, x^k, b)$, $T'_r = (k - 1, 1, a)$ which are linked as we have seen. (ii) In Lemma 4.2, $L_k = 1$, $\nu_1 = s_0 x^{k-1} \mu_1 - \Delta_1$ and $L_{k+1} = k$. If $\Delta = \Delta(\nu_1; s) \neq 0$ we have $T_s = (k + 1, \nu_1, \Delta)$, $T'_s = (k, \mu_1, \Delta_1)$ and $L_{k+1} + L_{(k+1)'} = k + 1 = (k + 1)' + 1$ so that T_s, T'_s are linked.

4.3 The Inductive Theorem and the Corresponding Algorithm

The elementary case $n = 1$, Example 4.5(ii), Lemmas 4.2 and 4.7 now yield

THEOREM 4.9 ([11, Theorems 3.13, 4.5]) For $n \geq 1$ and any sequence $s = s_0, \dots, s_{1-n}$ over D , we can construct a minimal solution μ for s .

PROOF. We induct on n . For $n = 1$, $\mu = (1, 0)$ is minimal if s is trivial and otherwise $\mu = (x, s_0)$ is. Let $n = 2$, $r = s_0$ and $s = r, s_{-1}$. If $\Delta_1 = \Delta(\mu_1; s) = 0$ then μ is as required. Otherwise $\Delta_1 \neq 0$ and s is non-trivial, so s is either pseudo-geometric or essential. In the first case, r is also pseudo-geometric and we can apply Lemma 4.2 to r and s_{-1} : we take $\mu = (s_0 x - s_{-1}, s_0^2)$. For the second case, r is trivial and $s_{-1} \neq 0$ so we take $\mu = (x^2, s_{-1})$. Moreover if we put $n' = 1$ then $L_n + L_{n'} = 2 = n' + 1$. Hence if s is non-trivial and $\Delta_1 = \Delta(x^2; s, s_{-2}) \neq 0$, we have linked triples $T_s = (2, x^2, \Delta_1)$, $T'_s = (1, 1, s_{-1})$.

Now let $n \geq 3$, $s = r, s_{1-n}$ and μ be our solution for r with linked triples T_r, T'_r if both $\underline{r} \neq 0$ and $\Delta_1 = \Delta(\mu_1; s) \neq 0$. Thus s is non-trivial; if s is pseudo-geometric, so is r and we apply Lemma 4.2 to r and s_{1-n} . Otherwise s is essential. If $\underline{r} = 0$ then $s_{1-n} \neq 0$. Put $\mu = (x^n, s_{1-n})$. Now $n' = n - 1$, $L_n + L_{n'} = n = n' + 1$ and $T'_s = (n', 1, s_{1-n})$ is a triple. For $\underline{r} \neq 0$, the inductive hypothesis and Lemma 4.7 apply to r, s_{1-n}, μ and linked triples T_r, T'_r to yield a new μ , and a linked T_s, T'_s if s is non-trivial and $\Delta(\mu_1; s, s_{-n}) \neq 0$. \square

REMARK 4.10 *The proof of Theorem 4.9 for minimal polynomials only does not require the fact that $x\mu_2 = [\mu_1 \cdot \underline{s}]$.*

COROLLARY 4.11 ([7, Theorem 2], cf. Corollary 3.9) *If $s = s_0, \dots, s_{1-n}$ is non-trivial and $\mu_1 \notin \text{Ann}(s, s_{-n})$ then $L_{n+1} = \max\{L_n, n+1 - L_n\}$.*

PROOF. As $\mu_1 \notin \text{Ann}(s, s_{-n})$, Theorem 4.9 implies that $\nu_1 \in \text{MP}(s, s_{-n})$ i.e. $L_{n+1} = |\nu_1|$. If $e_s \leq 0$, $L_{n+1} = L_n \geq n + 1 - L_n$. Otherwise $e_s > 0$ and $L_{n+1} = n + 1 - L_n > L_n$. \square

Next we derive the algorithm which follows from the constructive proof of Theorem 4.9. The constructions in Example 4.5(ii) and Lemma 4.2 bear some resemblance to Lemma 4.7, and pseudo-geometric sequences often become essential. Thus it is reasonable to try to fit these two cases into the format of Lemma 4.7 and to iterate.

First we rewrite Lemma 4.7 algorithmically using μ for the current solution, the variable Δ'_1 , updates for e and ν for the new solution. Here $2 \leq k \leq n-1$ and $s = s_0, \dots, s_{1-k}$ is essential:

LEMMA 4.7 (restated)

$$\begin{array}{ll} \Delta_1 \leftarrow \Delta(g_1; s_0, \dots, s_{-k}; \\ \text{if } \Delta_1 \neq 0 \text{ then if } e \leq 0 \text{ then} & [\nu \leftarrow (\Delta'_1 \mu - \Delta_1 x^{-e} \mu'; e \leftarrow 1 + e;] \\ & \text{else } [\nu \leftarrow \Delta'_1 x^e \mu - \Delta_1 \mu'; (\mu', \Delta'_1) \leftarrow (\mu, \Delta_1); e \leftarrow 1 - e;] \end{array}$$

(i) We observe how Lemma 4.7 (restated) reduces when $k = 0$ if we start with $\mu = (1, 0)$, $e = 1$, $\mu' = (0, -1)$ and $\Delta'_1 = 1$: we have $\Delta(\mu_1; s_0) = s_0$ and thus if $s_0 \neq 0$ we have $\nu = \Delta'_1 x^e \mu - \Delta_1 \mu' = x(1, 0) - s_0(0, -1) = (x, s_0)$ and the case $e \leq 0$ does not arise. We have the correct result when $s_0 \neq 0$; now $e = 0$, $\nu' = (1, 0)$ and $\Delta'_1 = s_0$.

(ii) Now let $k = 2$ and put $\mu = \nu$, $\mu' = \nu'$. We have $\Delta_1 = \Delta(\mu_1; s) = s_{-1}$. If $s_{-1} \neq 0$ and $e = 0$ i.e. $s_0 \neq 0$ we have $\nu = \Delta'_1 \mu - \Delta_1 x^{-e} \mu' = s_0(x, s_0) - s_{-1}(1, 0) = (s_0 x - s_{-1}, s_0^2)$ as desired. But if $s_0 = 0$ then s is essential and $\mu = (1, 0)$, giving $\nu = \Delta'_1 x^e \mu - \Delta_1 \mu' = x^2(1, 0) - s_{-1}(0, -1) = (x^2, s_{-1})$, $\nu' = (1, 0)$ and $\Delta'_1 = s_{-1}$, provided $e = 2$. So Lemma 4.7 (restated) behaves correctly when $k = 2$, provided $e = 2$ if $s_0 = 0$. We conclude that when $\Delta_1 \neq 0$, Lemma 4.7 (restated) applies if we initialise as in case (i) and $e \leftarrow 1 + e$ if $s_0 = 0$. Moreover s, s_{-2} will be essential, so that Lemma 4.7 (restated) can be reapplied.

Now replace ν by μ and ν' by μ' throughout. This requires a temporary variable T to avoid overwriting μ when $e > 0$. We factor out incrementing e , giving last statement $e \leftarrow 1 + e$.

If $\Delta_1 = 0$ then μ_1 remains unchanged and $e \leftarrow 1 + e$ since $k + 2 - 2|\mu_1| = 1 + e$. We can thus place $e \leftarrow 1 + e$ at the bottom of the loop, independently of Δ_1 , as in:

ALGORITHM 4.12 ([11, Algorithm 4.6], cf. [7, Algorithm 1])

Input: The $n \geq 1$ values of a sequence $s = s_0, \dots, s_{1-n}$ over D .

Output: A minimal solution μ for s .

```

 $\lceil \mu \leftarrow (1, 0); \mu' \leftarrow (0, -1); \Delta'_1 \leftarrow 1; e \leftarrow 1;$ 

for  $i \leftarrow 0$  to  $1 - n$  do

     $\lceil \Delta_1 \leftarrow \Delta(\mu_1; s_0, \dots, s_i);$ 

    if  $\Delta_1 \neq 0$  then if  $e \leq 0$  then  $\mu \leftarrow \Delta'_1 \mu - \Delta_1 x^{-e} \mu';$ 

        else  $\lceil T \leftarrow \mu; \mu \leftarrow \Delta'_1 x^e \mu - \Delta_1 \mu';$ 

             $(\mu', \Delta'_1) \leftarrow (T, \Delta_1); e \leftarrow -e; \rceil$ 

     $e \leftarrow 1 + e; \rceil$ 

return  $\mu.$ 

```

Note that after $s_0 = 0$ we have $e \geq 2$. We verify the remaining cases:

- (iii) s trivial; Algorithm 4.12 gives $\mu = (1, 0)$ as it should;
- (iv) $s = 0^{k-1}, s_{1-k}$ where $s_{1-k} \in \mathbb{F}^\times$; here $\mu = (1, 0)$, $e = (k-1) + 1 - 2|\mu_1| = k$ and $\Delta(\mu_1; s_0, \dots, s_{1-k}) = s_{1-k}$, Algorithm 4.12 gives $\mu = \Delta'_1 x^e \mu - \Delta_1 \mu' = x^k(1, 0) - s_{1-k}(0, -1) = (x^k, s_{1-k})$, $\mu' = (1, 0)$ and $\Delta'_1 = s_{1-k}$. This agrees with Example 4.5(ii) and moreover Lemma 4.7 can be reapplied.
- (v) $k \geq 2$ and s_0, \dots, s_{1-k} is pseudo-geometric; here $\mu = (s_0 x - s_{-1}, s_0^2)$, $\mu' = (1, 0)$ from (ii) above and $e = k + 1 - 2|\mu_1| = k - 1$. If $\Delta_1 = \Delta(\mu_1; s_0, \dots, s_{-k}) \neq 0$ then Algorithm 4.12 gives $\Delta'_1 x^e \mu - \Delta_1 \mu' = \Delta'_1 x^{k-1} \mu - \Delta_1 \mu'$ and $\mu = \mu'$, $\Delta'_1 = \Delta_1$, which agrees with Lemma 4.2, and Lemma 4.7 can be reapplied. Finally, if $\Delta_1 = 0$ then μ is unchanged.

We conclude that Algorithm 4.12 computes a minimal solution μ for s . Note that (i) we may suppress second components and compute μ_1 only as in [7]; (ii) Algorithm 4.12 is identical to [11, Algorithm 4.6] except that $\mu' \leftarrow (0, -x)$ has been replaced by $\mu' \leftarrow (0, -1)$, so that Algorithm 4.6, *loc. cit.* computes $x\mu_2$ instead of μ_2 .

REMARK 4.13 (INITIALISATION) In [1, Section 7.3], $(\sigma^{(0)}, \omega^{(0)}) = (1, 1)$ and $(\tau^{(0)}, \gamma^{(0)}) = (1, 0)$. This corresponds to the fact that $1 + s_1 x + \dots + s_n x^n \in \mathbb{F}[x]$ is used in the key equation [1, Equation 7.302]. Thus if $s = 0^n$ then $1 = 1/1$ obtains in [1], whereas $0 = 0/1$ obtains in our approach.

Our initialisation $\mu' = (0, -1)$ was chosen to yield the inductive bases of Theorem 4.9. In [7], we have the initialisation $'B(D) = 1'$, which corresponds to $\mu'_1 = 1$. Let Algorithm 4.12' denote Algorithm 4.12 using the initialisation $\mu'_1 = 1$. The reader may easily check that the first iteration of Algorithm 4.12' (with $\Delta_1 = s_v \neq 0$) produces $\mu_1 = x^n - s_v \in \text{MP}(s)$. As Lemmas 4.2, 4.7 apply to any $\mu_1 \in \text{MP}(s)$, Theorem 4.9 and hence Algorithm 4.12' also produces a minimal polynomial on subsequent iterations.

Table 1: Algorithm 4.12 for Example 4.3(ii)

s	Δ_1	Δ'_1	e_s	μ	μ'
	—	1	1	$(1, 0)$	$(0, -1)$
a	a	1	1	(x, a)	$(1, 0)$
a, b	b	1	0	$(ax - b, a^2)$	$(1, 0)$
a, b, c	$ac - b^2$	a	1	$ax(ax - b, a^2) - \Delta_1(1, 0)$	$(ax - b, a^2)$

PROPOSITION 4.14 (NORMALISED ALGORITHM 4.12) *If $D = \mathbb{F}$ is a field, $\rho = \Delta_1/\Delta'_1$ and μ of Algorithm 4.12 is updated via*

$$\mu \leftarrow \begin{cases} \mu - \rho x^{-e} \mu' & \text{if } e \leq 0 \\ x^{+e} \mu - \rho \mu' & \text{otherwise} \end{cases}$$

then Algorithm 4.12 produces a minimal solution μ for s with μ_1 monic.

PROOF. It suffices to show that the updating is well-defined and μ_1 is monic. Firstly, $\Delta'_1 = 1$ initially and Δ'_1 is either unchanged or replaced by $\Delta_1 \neq 0$. Thus ρ is well-defined. Secondly, μ_1 is monic for the base cases. Suppose that $s = s_0, \dots, s_{1-n}$ is essential and $e \leq 0$. Then $\text{lc}(\mu_1 - \rho x^{-e} \mu'_1) = \text{lc}(\mu_1)$ since $-e + L_{n'} = 2L_n - n - 1 + L_{n'} = L_n + n' - n < L_n$ as $L_n + L_{n'} = n' + 1$ and $n' < n$. Hence the updated μ_1 will be monic in this case. And *a fortiori* if $n \geq 2$ and s is either (i) geometric or (ii) essential and $e \geq 1$. \square

EXAMPLE 4.15 *Let $n \geq 2$ and $s = s_0, \dots, s_{1-n}$ be a geometric sequence over \mathbb{F} with common ratio $r = s_{-1}/s_0 \in \mathbb{F}$. Proposition 4.14 yields iterations (x, s_0) and $(x - r, s_0)$.*

EXAMPLE 4.16 (Cf. Example 3.2) *Let $s_i = \underline{s}_i$ where \underline{s} is as in Example 3.2. As in [15], $s = \alpha^5, \alpha^9, \alpha^4, 0, 0, \alpha^2$. Normalising Algorithm 4.12 gives the following table:*

s	Δ_1	Δ'_1	e_s	μ
—	—	1	1	$(1, 0)$
α^5	α^5	1	1	(x, α^5)
α^5, α^9	α^9	α^5	0	$(x + \alpha^4, \alpha^5)$
$\alpha^5, \alpha^9, \alpha^4$	α^{11}	α^5	1	$(x^2 + \alpha^4 x + \alpha^6, \alpha^5 x)$
$\alpha^5, \alpha^9, \alpha^4, 0$	α^2	α^{11}	0	$(x^2 + \alpha^{12} x + \alpha^7, \alpha^5 x + \alpha^{11})$
$\alpha^5, \alpha^9, \alpha^4, 0, 0$	α^{11}	α^{11}	1	$(x^3 + \alpha^{12} x^2 + \alpha^9 x + \alpha^4, \alpha^5 x^2 + \alpha^{11} x + \alpha^5)$
$\alpha^5, \alpha^9, \alpha^4, 0, 0, \alpha^2$	0	α^{11}	0	$(x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{13}, \alpha^5 x^2 + \alpha^2 x + \alpha^{10})$

For $r = s_0 \neq 0$, $\mu'(r) = \mu'(r, s_{-1}) = (1, 0)$; for $-5 \leq j \leq -2$ and $r = s_0, \dots, s_j$, $\mu'(r) = \mu'(r, s_j) = \mu(s_0, \dots, s_{2+j})$. Here $L_1 = L_2 = 1$, $L_3 = L_4 = 2$ and $L_5 = L_6 = 3$, which agrees with Theorem 3.7. Note that when $n = 2, 4, 6$ in this table and $i = 1, 2, 3$ in Example 3.2, $\mu = q^{(i)}/\text{lc}(q_1^{(i)})$.

4.4 A Worst-Case Analysis

Next we give a worst-case analysis of Algorithm 4.12. For $n \geq 1$ and $s = s_0, \dots, s_{1-n}$ define $\sigma_n = \sum_{i=0}^{1-n} L(s_0, \dots, s_i)$. The following identity and inequality seem to be new.

PROPOSITION 4.17 *If $s = s_0, \dots, s_{1-n}$ then $\sigma_n = L_n(n+1-L_n) \leq (n+1)^2/4$, with equality if and only if $n = 2L_n - 1$.*

PROOF. The equality is trivially true if $s = 0^n$. For the sequence $s = 0^{n-1}, s_v$ with $-v \geq 0$, we have $\sigma_n = n = n(n+1-n)$ as required. Suppose inductively that $n \geq 2$, s is non-trivial, the equality is true for $s = s_0, \dots, s_{1-n}$ and $t = s, s_{-n}$. If $\Delta(\mu_1; t) = 0$ then $L_{n+1} = L_n$ and by the inductive hypothesis

$$\sigma_{n+1} = \sigma_n + L_n = L_n(n+1-L_n) + L_n = L_n(n+2-L_n) = L_{n+1}(n+2-L_{n+1}).$$

If $\Delta(\mu_1; t) \neq 0$ we apply Lemma 4.2 or 4.7. If $n+1-L_n \leq L_n$ then $L_{n+1} = L_n$ and we have just seen that the result is true in this case. If $n+1-L_n > L_n$ then $L_{n+1} = n+1-L_n$ and by the inductive hypothesis,

$$\sigma_{n+1} = \sigma_n + (n+1-L_n) = L_n(n+1-L_n) + (n+1-L_n) = (L_n+1)(n+1-L_n)$$

Secondly, the right-hand side is $(n+1-L_n)(n+2-(n+1-L_n)) = (n+1-L_n)(L_n+1)$ which we have just seen is σ_{n+1} . This completes the inductive proof of equality.

For the inequality, we show that $4L_n(n+1-L_n) \leq (n+1)^2$. For integers a, b we have $4ab \leq (a+b)^2$, with equality if and only if $a = b$. Put $a = L_n$ and $b = n+1-L_n$. Then $a+b = n+1$, so that $4ab \leq (n+1)^2$, with equality if and only if $L_n = n+1-L_n$. \square

COROLLARY 4.18 (Cf. [4]) *Let $s = s_0, \dots, s_{1-n}$ be a sequence over D . Ignoring terms linear in n , the number of multiplications in Algorithm 4.12 to compute $\mu_1 \in \text{MP}(s)$ or a minimal solution μ for s is at most $cn^2/4$ where c is given by*

D	outputs	c
domain	μ_1	3
domain	solution μ	5
field	monic μ_1	2
field	solution μ , with monic μ_1	3.

PROOF. For $1 \leq k \leq n-1$, let $r = s_0, \dots, s_{1-k}$ and $\mu_1 \in \text{MP}(r)$. Then $\Delta(\mu_1; r, s_{-k})$ requires at most $L_k + 1$ multiplications and $\nu_1 \in \text{MP}(r, s_{-k})$ requires at most $L_k + 1$ if r is pseudo-geometric and $L_k + L_{k'} + 2$ otherwise. If r is essential then by construction $L_{k'} < L_{k'+1} = \dots = L_k$ so that ν_1 requires at most $3L_k + 2$ multiplications. Thus computing a minimal polynomial for $s = s_0, \dots, s_{1-n}$ requires at most $\sum_{k=1}^{n-1} (3L_k + 2) \leq 3n^2/4 + 2n$ multiplications by Proposition 4.17. If $(\mu_1, x\mu_2)$ is a solution for r then $|\mu_2| \leq L_k - 1$ and $\mu'_2 = 0$ or $|\mu'_2| \leq L_{k'} - 1$, so that we need at most $L_k + L_{k'}$ additional multiplications to obtain ν_2 . Ignoring linear terms, this gives at most $5n^2/4$ multiplications to obtain a solution for s . The remaining cases are similar. \square

4.5 An Identity for μ and μ'

We prove an identity satisfied by μ, μ' . This is our analogue of Identity (1) satisfied by partial quotients; see Theorem 3.1. First a non-zero scalar:

DEFINITION 4.19 *We define $\nabla_s \in D^\times$ using Algorithm 4.12 as follows: $\nabla_s = 1$ on initialisation. Let $\mu_1 \in \text{MP}(s)$ and $t = s, a$. If $\Delta_1 = \Delta(\mu_1; t) = 0$ put $\nabla_t = \nabla_s$; otherwise*

$$\nabla_t = \begin{cases} \Delta'_1 \nabla_s & \text{if } e_s \leq 0 \\ \Delta_1 \nabla_s & \text{otherwise.} \end{cases}$$

If D is the field of two elements then $\nabla_s = 1$ for any s . Suppose that $s = a, b, c$ with $a, b \in D^\times$ and $c \in D$ as in Example 4.3. After the first iteration, $\mu = (x, a)$, $\mu' = (1, 0)$ and $\nabla_a = a$. Next $\mu = (ax - b, a^2)$, $\mu' = (1, 0)$ and $\nabla_{a,b} = \Delta'_1 \nabla_a = a^2$ since $e_{a,b} = 0$. If $\Delta_1 = ac - b^2 \neq 0$ then $e_{a,b,c} = 1$ and $\nabla_{a,b,c} = \Delta_1 \nabla_{a,b} = (ac - b^2)a^2$.

PROPOSITION 4.20 (Cf. [1, Theorem 7.42]) *If μ, μ' are as in Algorithm 4.12 then*

$$\mu_2 \mu'_1 - \mu_1 \mu'_2 = \nabla_s.$$

PROOF. If s is trivial, $\mu = (1, 0)$, $\mu' = (0, -1)$ and $\mu_2 \mu'_1 - \mu_1 \mu'_2 = 0 \cdot 0 - 1 \cdot (-1) = 1$. Suppose inductively that $\mu_2 \mu'_1 - \mu_1 \mu'_2 = \nabla_s$ and $t = s, a$. If $\Delta_1 = 0$, there is nothing to prove. Otherwise let $e_s \leq 0$. By construction $\nu' = \mu'$ and

$$\begin{aligned} \nu_2 \nu'_1 - \nu_1 \nu'_2 &= (\Delta'_1 \mu_2 - \Delta_1 x^{-e} \mu'_2) \nu'_1 - (\Delta'_1 \mu_1 - \Delta_1 x^{-e} \mu'_1) \nu'_2 \\ &= (\Delta'_1 \mu_2 - \Delta_1 x^{-e} \mu'_2) \mu'_1 - (\Delta'_1 \mu_1 - \Delta_1 x^{-e} \mu'_1) \mu'_2 \\ &= \Delta'_1 (\mu_2 \mu'_1 - \mu_1 \mu'_2) = \Delta'_1 \nabla_s = \nabla_t \end{aligned}$$

whereas if $e_s \geq 1$ we have $\nu' = \mu$ and by construction

$$\begin{aligned} \nu_2 \nu'_1 - \nu_1 \nu'_2 &= (\Delta'_1 x^{+e} \mu_2 - \Delta_1 \mu'_2) \nu'_1 - (\Delta'_1 x^{+e} \mu_1 - \Delta_1 \mu'_1) \nu'_2 \\ &= (\Delta'_1 x^{+e} \mu_2 - \Delta_1 \mu'_2) \mu_1 - (\Delta'_1 x^{+e} \mu_1 - \Delta_1 \mu'_1) \mu_2 \\ &= \Delta_1 (\mu_2 \mu'_1 - \mu_1 \mu'_2) = \Delta_1 \nabla_s = \nabla_t. \quad \square \end{aligned}$$

If $\Delta_1 = ac - b^2 \neq 0$ in Example 4.3(ii), we have seen that $\nabla_{a,b,c} = a^2 \Delta_1$ and

$$\mu_2 \mu'_1 - \mu_1 \mu'_2 = a^3 x (ax - b) - (a^2 x^2 - abx - \Delta_1) a^2 = a^2 \Delta_1.$$

We have the following immediate consequence of Proposition 4.20.

COROLLARY 4.21 *If s is a finite sequence over \mathbb{F} then $\gcd(\mu_1, \mu_2) = \gcd(\mu_1, \mu'_1) = \gcd(\mu_2, \mu'_2) = 1$.*

The next useful consequence of Proposition 4.20 is worth stating separately. The proof is similar to that of Proposition 3.11 and is omitted.

PROPOSITION 4.22 *Let $f \in R^2$. If $m = f_2 \mu_1 - f_1 \mu_2$ and $m' = f_2 \mu'_1 - f_1 \mu'_2$ then*

$$\nabla_s f_1 = m' \mu_1 - m \mu'_1.$$

EXAMPLE 4.23 *For $s = 0^{n-1}, a$ as in Example 2.4(ii), $\mu = (x^n, a)$, $\mu' = (1, 0)$ and $\nabla_s = a$. For $f \in R^\times$, $m = f_2 \mu_1 - f_1 \mu_2 = f_2 x^n - f_1 a$, $m' = f_2 \mu'_1 - f_1 \mu'_2 = f_2$ and*

$$m' \mu_1 - m \mu'_1 = f_2 x^n - (f_2 x^n - f_1 a) = a f_1 = \nabla_s f_1.$$

5 Decomposition

We now turn to the set of annihilating polynomials of a finite sequence s over D (which may be $S|n$ for some infinite sequence S over a field).

We will characterise the annihilating polynomials which uses a pairing $R^2 \times R^2 \rightarrow R$. This pairing was suggested by Identities (2) and (3) of the Introduction. Even though our conclusions for pseudo-geometric sequences turn out to be a special case of those for essential sequences, we have treated each case separately as their proofs differ, and little would be gained by combining their proofs in one place. Moreover the simpler pseudo-geometric case acts as a precursor to the remaining case. For essential sequences, the integer n' and the identity $L_n + L_{n'} = n' + 1$ are vital. In each case, we characterise the elements of $\text{Ann}(s)$ using the pairing and show that if we restrict to annihilators of degree at most n , our decomposition is unique and we can describe the set of solutions.

These proofs are valid once we know either a minimal polynomial or a 'minimal system' (see Definition 5.8) for the original finite sequence i.e. they do not depend on the provenance of the minimal polynomial.

5.1 A Pairing

Propositions 3.11 and 4.20 suggest the following definition:

DEFINITION 5.1 *For a sequence s we define a pairing $\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_s : R^2 \times R^2 \rightarrow R$ by*

$$\langle f, g \rangle = f_2 g_1 - f_1 g_2$$

where $x f_2 = [f_1 \cdot \underline{s}]$ and similarly for g_2 .

For s, g, t and h as in Lemma 2.6, the proof of Lemma 2.6 shows that $\langle g, h \rangle_t \neq 0$ and $|\langle g, h \rangle_t| = |g| + |h| - n - 1 \geq 0$.

From Corollary 3.10 and Proposition 3.11 we have $(-1)^{i-1} f_1 = \langle f, q' \rangle q_1 - \langle f, q \rangle q'_1$. We can restate Proposition 4.20 as $\langle \mu, \mu' \rangle = \nabla_s$ and Proposition 4.22 as

$$\nabla_s f_1 = \langle f, \mu' \rangle \mu_1 - \langle f, \mu \rangle \mu'_1.$$

5.2 Geometric Sequences. II

Throughout this subsection, $n \geq 1$ and $s = s_0, \dots, s_{1-n}$ is a pseudo-geometric sequence over D . We assume that $\lambda \in R^2$ is a minimal solution for s , $L_n = \dots = L_1 = |\lambda_1| = 1$ and $\lambda' = (1, 0)$, so that $\lambda_2 = \langle \lambda, \lambda' \rangle = \nabla \in D^\times$. For example, if λ is obtained via Proposition 3.5 then $\lambda = ((x - r)/S_0, 1)$ and $\nabla = 1$. If λ is obtained from Theorem 4.9 then $\lambda_1 = x$ and $\nabla = s_0$ if $s_{-1} = 0$; otherwise $\lambda_1 = s_0 x - s_{-1}$ and $\nabla = s_0^2$. In both cases we have $\nabla f_1 = \langle f, \lambda' \rangle \lambda_1 - \langle f, \lambda \rangle \lambda'_1$.

5.2.1 Annihilating Polynomials

LEMMA 5.2 *Let $f_1 \in \text{Ann}(s)^\times$ and $x f_2 = [f_1 \cdot \underline{s}]$. If $\varphi \in R$, $g_1 = f_1 - \varphi$, $x g_2 = [g_1 \cdot \underline{s}]$ and $|\varphi| \leq |f_1| - n$ then (i) $|g_1| = |f_1|$, $g_1 \in \text{Ann}(s)^\times$ and $g_2 = f_2$; (ii) $\langle g, f \rangle = \varphi f_2$.*

PROOF. (i) Firstly $|\varphi| \leq |f_1| - n \leq |f_1| - 1$, so $|g_1| = |f_1|$. Since $f_1 \in \text{Ann}(s)$ we can write $f_1 \cdot \underline{s} = F + x f_2$ where $v(F) \leq |f_1| - n = |g_1| - n$. Then

$$g_1 \cdot \underline{s} = (f_1 - \varphi) \cdot \underline{s} = F + x f_2 - \varphi \cdot \underline{s}$$

and $v(\varphi \cdot \underline{s}) = |\varphi| + v = |\varphi| \leq |f_1| - n = |g_1| - n$ since $L_1 = 1$ implies that $v = 0$. Therefore $v(g_1 \cdot \underline{s} - x f_2) \leq |g_1| - n$, $g_1 \in \text{Ann}(s)^\times$ and $g_2 = f_2$. (ii) From Part (i) and the definition $\langle g, f \rangle = g_2 f_1 - g_1 f_2 = f_2 f_1 - (f_1 - \varphi) f_2 = \varphi f_2$. \square

PROPOSITION 5.3 *Let $f \in R^2$ and $x f_2 = [f_1 \cdot \underline{s}]$. If $m = \langle f, \lambda \rangle$ and $m' = \langle f, \lambda' \rangle$ then $m = f_2 \lambda_1 - \nabla f_1$, $m' = f_2$ and $|f_2| = |f_1| - 1$. Further*

- (i) $f_1 \in \text{Ann}(s)^\times$ if and only if $|m'| = |f_1| - 1$ and $|m| \leq |f_1| - n$;
- (ii) if $f_1 \in \text{Ann}(s)^\times$ and $|f_1| \leq n$ then $m \in D$.

PROOF. Since $\lambda_2 = \nabla$, $\lambda_1 \cdot \underline{s} = M + x \nabla$ where $v(M) \leq 1 - n \leq 0$. (i) For any $f_1 \in R^\times$, $m = \langle f, \lambda \rangle = f_2 \lambda_1 - f_1 \nabla$ and $m' = \langle f, \lambda' \rangle = f_2$. We have $|m'| = |f_2| = v + |f_1| - 1 = |f_1| - 1$. Let $f_1 \in \text{Ann}(s)^\times$ so that $f_1 \cdot \underline{s} = F + x f_2$ where $v(F) \leq |f_1| - n$. Then

$$f_1 \cdot (M + x \nabla) = f_1 \cdot (\lambda_1 \cdot \underline{s}) = \lambda_1 \cdot (f_1 \cdot \underline{s}) = \lambda_1 \cdot (F + x f_2)$$

$x m = x(f_2 \lambda_1 - \nabla f_1) = f_1 \cdot M - \lambda_1 \cdot F$ and $|m| + 1 \leq \max\{v(f_1 \cdot M), v(\lambda_1 \cdot F)\} \leq |f_1| + 1 - n$ as claimed. Conversely, suppose that $|m'| = |f_1| - 1$ and $|m| \leq |f_1| - n$. We claim that $m' \lambda_1 \in \text{Ann}(s)$:

$$(m' \lambda_1) \cdot \underline{s} = m' \cdot (M + \nabla x) = m' \cdot M + x \nabla m'$$

and $v(m' \cdot M) \leq |m'| + 1 - n = |m \lambda_1| - n$. We have $m = f_2 \lambda_1 - \nabla f_1 = m' \lambda_1 - \nabla f_1$, so $\nabla f_1 = m' \lambda_1 - m$. Consider $g_1 = \nabla f_1$: $|g_1| = |f_1|$ and $|m| \leq |f_1| - n = |m'| + 1 - n = |m' \lambda_1| - n$ since $|m| \leq |f_1| - n = |g_1| - n$. So $g_1 \in \text{Ann}(s)$ by Lemma 5.2 and hence $f_1 \in \text{Ann}(s)^\times$. (ii) This is immediate. \square

COROLLARY 5.4 (i) $\nabla \text{Ann}(s)^\times \subseteq \{\varphi' \lambda_1 - \varphi : \varphi' \neq 0, |\varphi| \leq |\varphi'| + 1 - n\} \subseteq \text{Ann}(s)$;
(ii) $\nabla \text{MP}(s) \subseteq \{\varphi' \lambda_1 - \varphi : \varphi' \in D^\times, |\varphi| \leq 1 - n\} \subseteq \text{MP}(s)$;
(iii) if $n \geq 2$ then $\nabla \text{MP}(s) \subseteq \{\varphi' \lambda_1 : \varphi' \in D^\times\} \subseteq \text{MP}(s)$.

PROOF. (i) If $f_1 \in \text{Ann}(s)^\times$ then $\nabla f_1 = m' \lambda_1 - m$ where $|m'| = |f_2| = |f_1| - 1 \geq 0$ and $|m| \leq |f_1| - n = |m'| + 1 - n$ by Proposition 5.3. If $\varphi' \neq 0$ and $|\varphi| \leq |\varphi'| + 1 - n$ then $\varphi' \lambda_1 - \varphi \in \text{Ann}(s)^\times$ by Lemma 5.2. (ii), (iii) These are immediate. \square

5.2.2 Solutions

We apply the results of the previous subsection to finding solutions for a pseudo-geometric sequence; this is a precursor to the discussion of solutions for essential sequences in Subsection 5.3.2.

LEMMA 5.5 *Let $\varphi, \varphi' \in \mathbb{R}$. If $g_1 = \varphi' \lambda_1 - \varphi$, $0 \leq |\varphi'| \leq n - 1$, $\varphi \in \mathbb{D}$ and $x g_2 = [g_1 \cdot \underline{s}]$ then $g_2 = \varphi' \lambda_2 = \nabla \varphi'$, $\nabla \varphi = \langle g, \lambda \rangle$ and $\nabla \varphi' = \langle g, \lambda' \rangle$.*

PROOF. We have $\lambda_1 \cdot \underline{s} = M + x \lambda_2$ where $v(M) \leq 1 - n$ and

$$g_1 \cdot \underline{s} = \varphi' \cdot (\lambda_1 \cdot \underline{s}) - \varphi \cdot \underline{s} = \varphi' \cdot (M + x \lambda_2) - \varphi \cdot \underline{s} = \varphi' \cdot M - \varphi \cdot \underline{s} + x \varphi' \lambda_2.$$

Further, $v(\varphi' \cdot M) \leq |\varphi'| + 1 - n \leq 0$ by hypothesis and $v(\varphi \cdot \underline{s}) = v = 0$ since $\varphi \in \mathbb{D}$. Thus $v(\varphi' \cdot M - \varphi \cdot \underline{s}) \leq 0$ and $g_2 = \varphi' \lambda_2 = \nabla \varphi'$. We have

$$\langle g, \lambda \rangle = g_2 \lambda_1 - g_1 \lambda_2 = \nabla \varphi' \lambda_1 - (\varphi' \lambda_1 - \varphi) \nabla = \nabla \varphi$$

and $\langle g, \lambda' \rangle = g_2 \lambda'_1 - g_1 \lambda'_2 = g_2 = \nabla \varphi'$. □

COROLLARY 5.6 *Let $f_1 \in \text{Ann}(s)$, $|f_1| \leq n$ and $m' = \langle f, \lambda' \rangle$, $m = \langle f, \lambda \rangle$. Then*

(i) (uniqueness) if $\nabla f_1 = \varphi' \lambda_1 - \varphi$ where $0 \leq |\varphi'| \leq n - 1$ and $\varphi \in \mathbb{D}$ then $\varphi = m$ and $\varphi' = m'$;

(ii) $\nabla f_2 = m' \lambda_2 - m \lambda'_2$.

PROOF. (i) Applying Lemma 5.5 to $g_1 = \nabla f_1 = \varphi' \lambda_1 - \varphi$ gives $\nabla \varphi = \langle g, \lambda \rangle = \nabla \langle f, \lambda \rangle = \nabla m$. Hence $\varphi = m = f_2$ and similarly $\varphi' = m' = f_2 \lambda_1 - \nabla f_1$. (ii) We have $\nabla f_2 = m' \lambda_2 - m \lambda'_2$ since $m' = f_2$, $\lambda_2 = \nabla$ and $\lambda'_2 = 0$. □

Thus if s is a geometric sequence over \mathbb{F} , μ, ∇ are obtained from Algorithm 4.12 and $\mu' = (1, 0)$ then the minimal solutions for s are

$$\{(\varphi' \mu - \varphi, \varphi') : \varphi' \in \mathbb{F}^\times, |\varphi| \leq 1 - n\}.$$

Also if $S_0 \neq 0$ and $n \in [1, n_2)$ we may take $\lambda = (a_1, 1)$, $\lambda' = (1, 0)$ and $\nabla = 1$. For example, from Corollary 5.4

COROLLARY 5.7 *Let S be an infinite geometric sequence over \mathbb{F} , $r = S_{-1}/S_0$, $n \in [1, n_2)$ and $s = S|n$. The minimal solutions for s are*

$$\{(\varphi'(x - r) - \varphi, \varphi') : \varphi' \in \mathbb{F}^\times, |\varphi| \leq 1 - n\}.$$

5.3 Essential Sequences. II

When s is essential, more information is available for decomposition. Informally, we have a pair of linked triples, their second components and $\nabla \in D^\times$, all related by the pairing of Definition 5.1.

DEFINITION 5.8 *Let $n \geq 2$ and $s = s_0, \dots, s_{1-n}$ be an essential sequence over D . A minimal system for s is a 5-tuple $(\lambda, n', \lambda', \langle, \rangle_s, \nabla)$ consisting of*

- (i) *a minimal solution $\lambda \in R^2$ for s and $\lambda_1 \notin \text{Ann}(s, s_{-n})$;*
- (ii) *$n' = \max_{1 \leq j < n} \{j : L_j < L_n\}$ and $s' = s_0, \dots, s_{1-n'}$;*
- (iii) *a minimal solution $\lambda' \in R^2$ for s' , $\lambda'_1 \notin \text{Ann}(s', s_{-n'})$ and $L_n + L_{n'} = n' + 1$;*
- (iv) *the pairing $\langle, \rangle_s : R^2 \times R^2 \rightarrow R$ of Definition 5.1;*
- (v) *$\nabla = \langle \lambda, \lambda' \rangle_s \in D^\times$.*

From Theorem 3.1 and Corollary 3.10, $(q, n_i - 1, q', \langle, \rangle_{S|n}, (-1)^{i-1})$ is a minimal system for $S|n$ if $n \in [n_i, n_{i+1})$ and $S|n$ is essential. We have seen that if (n, μ_1, Δ) and (n', μ'_1, Δ') are linked triples for s then $(\mu, n', \mu', \langle, \rangle_s, \nabla_s)$ is a minimal system for s by Theorem 4.9, Definition 4.19 and Proposition 4.20.

N.B. Throughout this subsection, $n \geq 2$, s is a sequence over D and $(\lambda, n', \lambda', \langle, \rangle_s, \nabla)$ is a minimal system for $s = s_0, \dots, s_{1-n}$. We put $\langle, \rangle = \langle, \rangle_s$, $L = L_n$ and $L' = L_{n'}$.

As we have already seen in Propositions 3.11 and 4.20(ii), for any $f \in R^2$ we have

$$\nabla f_1 = \langle f, \lambda' \rangle \lambda_1 - \langle f, \lambda \rangle \lambda'_1.$$

5.3.1 Annihilating Polynomials

LEMMA 5.9 *If $f_1 \in \text{Ann}(s)^\times$, $\varphi \in R$, $g_1 = f_1 - \varphi \lambda'_1$ and $|\varphi| \leq |f_1| + L - n - 1$ then*

- (i) *$|g_1| = |f_1|$, $g_1 \in \text{Ann}(s)^\times$ and $g_2 = f_2 - \varphi \lambda'_2$;*
- (ii) *$\langle g, f \rangle = \varphi \langle f, \lambda' \rangle$.*

PROOF. (i) Firstly $|g_1| = |f_1|$ since $n' < n$ implies that

$$|\varphi \lambda'_1| = |\varphi| + L' \leq |f_1| + L - n - 1 + L' = |f_1| - n + n' \leq |f_1| - 1.$$

Since $f_1 \in \text{Ann}(s)$ we can write $f_1 \cdot \underline{s} = F + x f_2$ where $v(F) \leq |f_1| - n = |g_1| - n$ and $\lambda'_1 \cdot \underline{s}' = M' + x \lambda'_2$ where $v(M') \leq L' - n' = 1 - L$. Put $N' = \lambda'_1 \cdot (\underline{s} - \underline{s}')$. Then $v(N') \leq L' - n' = 1 - L$ and so $\lambda'_1 \cdot \underline{s} = N' + M' + x \lambda'_2$ where $v(N' + M') \leq 1 - L$. Thus

$$g_1 \cdot \underline{s} = (f_1 - \varphi \lambda'_1) \cdot \underline{s} = F + x f_2 - \varphi \cdot (N' + M' + x \lambda'_2) = F - \varphi \cdot (N' + M') + x (f_2 - \varphi \lambda'_2).$$

Now $v(\varphi \cdot (N' + M')) \leq |\varphi| + 1 - L \leq |f_1| + L - n - 1 + 1 - L = |f_1| - n = |g_1| - n$, $g_1 \in \text{Ann}(s)^\times$ and $g_2 = f_2 - \varphi \lambda'_2$. (ii) From Part (i) $\langle g, f \rangle = (f_2 - \varphi \lambda'_2) f_1 - (f_1 - \varphi \lambda'_1) f_2 = \varphi \langle f, \lambda' \rangle$. \square

THEOREM 5.10 *Let $f \in R^2$. If $m = \langle f, \lambda \rangle$ and $m' = \langle f, \lambda' \rangle$ then*

- (i) $f_1 \in \text{Ann}(s)^\times$ *if and only if* $|m'| = |f_1| - L$ *and* $|m| \leq |f_1| + L - n - 1$;
- (ii) *if* $f_1 \in \text{Ann}(s)^\times$ *then* $|m| + L' \leq |f_1| - 1$. *If in addition* $|f_1| \leq n$ *then* $|m'| \leq n - L$ *and* $|m| \leq L - 1$.

PROOF. First write $\lambda_1 \cdot \underline{s} = M + x \lambda_2$ where $v(M) \leq L - n \leq 0$. (i) Let $f_1 \in \text{Ann}(s)^\times$, so that $f_1 \cdot \underline{s} = F + x f_2$ where $v(F) \leq |f_1| - n$. Then

$$f_1 \cdot (M + x \lambda_2) = f_1 \cdot (\lambda_1 \cdot \underline{s}) = \lambda_1 \cdot (f_1 \cdot \underline{s}) = \lambda_1 \cdot (F + x f_2)$$

$x m = x (f_2 \lambda_1 - f_1 \lambda_2) = f_1 \cdot M - \lambda_1 \cdot F$ and $|m| + 1 \leq \max\{|f_1| + v(M), L + v(F)\} \leq |f_1| + L - n$. Hence

$$|m| + L' \leq |f_1| + L - n - 1 + L' = |f_1| + n' - n \leq |f_1| - 1$$

as $n' < n$. We have $\nabla f_1 = m' \lambda_1 - m \lambda'_1$, so $|m'| = |f_1| - L$. Conversely, if $|m'| = |f_1| - L$ then $m' \lambda_1 \in \text{Ann}(s)$, for

$$(m' \lambda_1) \cdot \underline{s} = m' \cdot (M + x \lambda_2) = m' \cdot M + x m' \lambda_2$$

and $v(m' \cdot M) \leq |m'| + L - n = |m' \lambda_1| - n$. We claim that $\nabla f_1 = m' \lambda_1 - m \lambda'_1 \in \text{Ann}(s)$. From Lemma 5.9, it suffices to check that $|m| \leq |m' \lambda_1| + L - n - 1$. But $|m'| = |f_1| - L$, so $|m| \leq |f_1| + L - n - 1$ suffices, and this is true by hypothesis. We conclude that $\nabla f_1 \in \text{Ann}(s)$ and hence so is f_1 . (ii) The first sentence was proved in Part (i); we also have $|m'| = |f_1| - L \leq n - L$ and $|m| \leq |f_1| + L - n - 1 \leq L - 1$. \square

Recall that for any sequence $s = s_0, \dots, s_{1-n}$ over D , $e_s = n + 1 - 2L_n \in \mathbb{Z}$.

COROLLARY 5.11 (Cf. [7])

- (i) $\nabla \text{Ann}(s)^\times \subseteq \{\varphi' \lambda_1 - \varphi \lambda'_1 : \varphi' \neq 0, |\varphi| \leq |\varphi'| - e_s\} \subseteq \text{Ann}(s)^\times$;
- (ii) $\nabla \text{MP}(s) \subseteq \{\varphi' \lambda_1 - \varphi \lambda'_1 : \varphi' \in D^\times, |\varphi| \leq -e_s\} \subseteq \text{MP}(s)$;
- (iii) *if* $2L \leq n$ *then* $\nabla \text{MP}(s) \subseteq \{\varphi' \lambda_1 : \varphi' \in D^\times\} \subseteq \text{MP}(s)$.

Moreover if ∇ is a unit of D (for example if D is a field) the inclusions are equalities.

PROOF. (i) If $f_1 \in \text{Ann}(s)^\times$ then $\nabla f_1 = m' \lambda_1 - m \lambda'_1$ where $|m'| = |f_1| - L$ and $|m| \leq |f_1| + L - n - 1 = |m'| - e_s$ by Theorem 5.10. If $\varphi' \neq 0$ and $|\varphi| \leq |\varphi'| - e_s$ then $\varphi' \lambda_1 - \varphi \lambda'_1 \in \text{Ann}(s)^\times$ by Lemma 5.9. (ii) If $f_1 \in \text{Ann}(s)$ and $|f_1| = L$ then by Theorem 5.10, $|m'| = 0$. If $f_1 = \varphi' \lambda_1 - \varphi \lambda'_1$, $\varphi' \in D^\times$ and $|\varphi| \leq -e_s$ then $f_1 \in \text{Ann}(s)$ and $|f_1| = |\lambda_1| = L$ by Lemma 5.9. Part (iii) is an immediate consequence of (ii). If $f_1 \in \text{Ann}(s)^\times$ and ∇ is a unit of D then $f_1/\nabla \in \text{Ann}(s)^\times$ and hence $f_1 \in \nabla \text{Ann}(s)^\times$. \square

Thus if $e_s \leq 0$ we have $\lambda_1 - \lambda'_1 \in \text{MP}(s)$, as is well-known for sequences over a field. From Theorem 3.7 and Corollary 5.11 we have

COROLLARY 5.12 (Cf. [9, Theorem 1]) Let S be an infinite sequence over \mathbb{F} , $n \in [n_i, n_{i+1})$ and $q = q^{(i)}$, $q' = q^{(i-1)}$. If $s = S|n$ is essential then

$$\text{Ann}(s)^\times = \{\varphi' q_1 - \varphi q'_1 : \varphi' \neq 0, |\varphi| \leq |\varphi'| - e_s\}, \text{MP}(s) = \{\varphi' q_1 - \varphi q'_1 : \varphi' \in \mathbb{F}^\times, |\varphi| \leq -e_s\}.$$

5.3.2 Solutions

Next we look at solutions i.e. pairs (f_1, f_2) with $f_1 \in \text{Ann}(s)^\times$ and $x f_2 = [f_1 \cdot \underline{s}]$.

LEMMA 5.13 Let $\varphi, \varphi' \in R$. If $g_1 = \varphi' \lambda_1 - \varphi \lambda'_1$, $0 \leq |\varphi'| \leq n - L$ and $|\varphi| \leq L - 1$ then (i) $g_2 = \varphi' \lambda_2 - \varphi \lambda'_2$; (ii) $\nabla \varphi = \langle g, \lambda \rangle$ and $\nabla \varphi' = \langle g, \lambda' \rangle$.

PROOF. (i) We have $\lambda_1 \cdot \underline{s} = M + x \lambda_2$ and $\lambda'_1 \cdot \underline{s}' = M' + x \lambda'_2$ where $v(M) \leq L - n$ and $v(M') \leq L' - n' = 1 - L$. Write $\underline{s} = (\underline{s} - \underline{s}') + \underline{s}'$ so that $v(\underline{s} - \underline{s}') \leq -n'$ and put $N' = \lambda'_1 \cdot (\underline{s} - \underline{s}')$. This gives

$$\begin{aligned} g_1 \cdot \underline{s} &= (\varphi' \lambda_1 - \varphi \lambda'_1) \cdot \underline{s} = \varphi' \cdot (M + x \lambda_2) - \varphi \lambda'_1 \cdot ((\underline{s} - \underline{s}') + \underline{s}') \\ &= \varphi' \cdot (M + x \lambda_2) - \varphi \cdot N' - \varphi \cdot (M' + x \lambda'_2) \\ &= \varphi' \cdot M - \varphi \cdot N' - \varphi \cdot M' + x (\varphi' \lambda_2 - \varphi \lambda'_2). \end{aligned}$$

Further, $v(\varphi' \cdot M) \leq |\varphi'| + L - n \leq 0$ by hypothesis and similarly $v(\varphi \cdot M') \leq 0$. Now

$$v(\varphi \cdot N') = |\varphi| + |\lambda'_1| + v(\underline{s} - \underline{s}') \leq |\varphi| + L' - n' = |\varphi| + 1 - L \leq 0$$

as $|\varphi| \leq L - 1$. Thus $v(\varphi' \cdot M - \varphi \cdot N' - \varphi \cdot M') \leq 0$ and $g_2 = \varphi' \lambda_2 - \varphi \lambda'_2$. (ii) We have

$$\begin{aligned} \langle g, \lambda \rangle &= g_2 \lambda_1 - g_1 \lambda_2 = (\varphi' \lambda_2 - \varphi \lambda'_2) \lambda_1 - (\varphi' \lambda_1 - \varphi \lambda'_1) \lambda_2 \\ &= \varphi (\lambda_2 \lambda'_1 - \lambda_1 \lambda'_2) = \nabla \varphi. \end{aligned}$$

Similarly $\langle g, \lambda' \rangle = g_2 \lambda'_1 - g_1 \lambda'_2 = \varphi' (\lambda_2 \lambda'_1 - \lambda_1 \lambda'_2) = \nabla \varphi'$. \square

COROLLARY 5.14 Let f be a solution for s , $|f_1| \leq n$ and $m' = \langle f, \lambda' \rangle$, $m = \langle f, \lambda \rangle$.

(i) (uniqueness) If $\nabla f_1 = \varphi' \lambda_1 - \varphi \lambda'_1$ where $0 \leq |\varphi'| = |f_1| - L$ and $|\varphi| \leq L - 1$ then $\varphi = m$ and $\varphi' = m'$;

(ii) $\nabla f_2 = m' \lambda_2 - m \lambda'_2$;

(iii) (degree bound) if $\lambda'_2 \neq 0$ then $|m| + |\lambda'_2| \leq |f_2| - 1$ and $|f_2| = |m'| + |\lambda_2|$.

PROOF. (i) Applying Lemma 5.13 to $g_1 = \nabla f_1 = \varphi' \lambda_1 - \varphi \lambda'_1$ gives $\nabla m = \nabla \langle f, \lambda \rangle = \langle \nabla f, \lambda \rangle = \langle g, \lambda \rangle = \nabla \varphi$. Therefore $\varphi = m$ and $\varphi' = m'$.

(ii) We know from Theorem 5.10 that $\nabla f_1 = m' \lambda_1 - m \lambda'_1$ where $|m'| \leq n - L$ and $|m| \leq L - 1$. Hence Lemma 5.13 implies that $\nabla f_2 = m' \lambda_2 - m \lambda'_2$.

(iii) We have $\lambda' \in \text{Ann}(s')$ and if s' is trivial then $\lambda' = (c, 0)$ for some $c \in D^\times$. As $\lambda'_2 \neq 0$, s' is non-trivial so $1 - n' \leq v(s') \leq 0$ and therefore $v(s') = v$. From Theorem 5.10, $|m| + L' \leq |f_1| - 1$, so

$$|m| + |\lambda'_2| = |m| + (v(s') + |\lambda'_1| - 1) = |m| + v + L' - 1 \leq |f_1| - 1 + v - 1 = |f_2| - 1.$$

From Part (ii) we have $\nabla f_2 = m' \lambda_2 - m \lambda'_2$, so $|f_2| = |m'| + |\lambda_2|$. \square

The final result of this section on solutions is a simple consequence of Corollary 5.14.

COROLLARY 5.15 (Cf. [7]) If $n \geq 2$, $s = s_0, \dots, s_{1-n}$ is an essential sequence and Σ denotes the solutions $\{(f_1, f_2) : f_1 \in \text{Ann}(s), 0 \leq |f_1| \leq n\}$ then

$$\nabla \Sigma \subseteq \{\varphi' \lambda - \varphi \lambda', 0 \leq |\varphi'| \leq n - L, |\varphi| \leq |\varphi'| - e_s\} \subseteq \Sigma$$

and if ∇ is a unit of D (for example if D is a field) the inclusions are equalities.

We leave the corresponding result for minimal solutions to the interested reader.

6 Some Applications of Decomposition

We give some applications of the results from the previous sections. As usual, $n \geq 1$, $s = s_0, \dots, s_{1-n}$ is non-trivial and μ, μ' are obtained using Algorithm 4.12 or, if D is a field \mathbb{F} , using the Normalised Algorithm 4.12. We put $L = L(s)$.

6.1 Sequences over a Field

We prove several gcd-related results, relate partial quotients to μ_1, μ'_1 and count the number of solutions when $|\mathbb{F}| < \infty$. Firstly a partial converse to Proposition 2.8(ii).

COROLLARY 6.1 If $2L \leq n$, $f_1 \in \text{Ann}(s)^\times$ and $|f_1| \leq n - L$ then

- (i) $\nabla_s f = m' \mu$;
- (ii) if in addition $\gcd(f_1, f_2) = 1$ then $m' \in \mathbb{F}^\times$ i.e. $f_1 \in \text{MP}(s)$.

PROOF. (i) Since $L \leq n - L$, such an f_1 can exist. Proposition 5.3 or Theorem 5.10 imply that $\nabla_s f_1 = m' \mu_1 - m \mu'_1$ where $|m'| = |f_1| - L \geq 0$ and $|m| \leq |f_1| + L - n - 1 \leq -1$, so $\nabla_s f_1 = m' \mu$. Since $|f_1| \leq n$, we also have $\nabla_s f_2 = m' \mu_2 - m \mu'_2$ from Corollary 5.4 or Corollary 5.14 i.e. $\nabla_s f = m' \mu$. (ii) By Corollary 4.21, $\gcd(\mu_1, \mu_2) = 1$, so $\nabla_s = \gcd(\nabla_s f_1, \nabla_s f_2) = \gcd(m' \mu_1, m' \mu_2) = m'$. Thus $m' \in \mathbb{F}^\times$ and $|f_1| = |\mu_1| = L$. \square

The example after Proposition 2.8 shows that the condition $|f_1| \leq n - L$ is necessary. Secondly, one may show directly that if $f_1, g_1 \in \text{Ann}(s)^\times$ and $|f_1| + |g_1| \leq n$ then $\langle f, g \rangle = 0$; see [11, Corollary 3.25]. This gives another proof of Corollary 6.1.

COROLLARY 6.2 (Cf. [5, p. 439-444]). Let S be a linear recurring sequence over \mathbb{F} , $\text{Id}_S = g_1 \mathbb{F}[x]$ where g_1 is monic, $n \geq 2|g_1|$ and $s = S|n$. Then

- (i) g is a minimal solution for s and any minimal solution of s is $c g$ for some $c \in \mathbb{F}^\times$;
- (ii) $\underline{S} = [g_1 \cdot \underline{S}]/g_1$ and S is determined by $S_0, \dots, S_{2|g_1|-1}$;
- (iii) if i is the first index such that $b_{i+1} = 0$ in obtaining the partial quotients of \underline{S} , then $g = q^{(i)}/\text{lc}(q_1^{(i)})$.

PROOF. (i) Firstly, g is a solution for $s = S|n$. As g_1 is a minimal polynomial of S , $\gcd(g_1, g_2) = 1$ and $xg_2 = [g_1 \cdot \underline{S}] = [g_1 \cdot \underline{s}]$ by Lemma 3.3 since $n \geq |g_1|$. As $|g_1| \leq n - |g_1|$, g_1 is a minimal solution for s by Corollary 6.1. Further $e_s > 0$ so any minimal solution for s is $c g$ where $c \in \mathbb{F}^\times$ by Corollary 5.4 or 5.11. (ii) We have $\underline{S} = [g_1 \cdot \underline{S}]/g_1 = [g_1 \cdot \underline{s}]/g_1 = xg_2/g_1$.

Since g_1 is uniquely determined by $s_0, \dots, s_{2|g_1|-1}$, so are g_2 and S . (iii) If s is geometric, this is Example 4.15. Suppose that s is essential and put $q = q^{(i)}$, $q' = q^{(i-1)}$. We have $n_{i+1} = \infty$ since $\underline{s} \in \mathbb{F}(x)$ and $n_i = |q'_1| + |q_1| < 2|q_1| = 2L \leq n < n_{i+1}$. From Theorem 3.7, q is a minimal solution for s and g is the unique monic solution of s by Corollary 5.11 since $e_s > 0$ and $L \leq 2L \leq n$. \square

Instances of Part(iii) of Corollary 6.2 were given in Example 4.16.

COROLLARY 6.3 *Suppose that f is a solution for s such that $|f_1| \leq n$ and let $m = \langle f, \mu \rangle$, $m' = \langle f, \mu' \rangle$. Then $\gcd(m, m') = \gcd(f_1, f_2)$.*

PROOF. By definition, $m = f_2\mu_1 - f_1\mu_2$ and $m' = f_2\mu'_1 - f_1\mu'_2$ so that if $d|f_1, f_2$ then $d|m, m'$. We also know that $\nabla f_1 = m'\mu_1 - m\mu'_1$ by Proposition 4.20. Corollary 5.14 implies that $\nabla f_2 = m'\mu_2 - m\mu'_2$ since $|f_1| \leq n$. Hence if $d|m, m'$ then $d|f_1, f_2$. \square

For the next result, \mathbb{F}_q is a finite field with $q < \infty$ elements. If $d \geq 0$, the number of polynomials with coefficients in \mathbb{F}_q of degree d is $N_d = (q-1)q^d$ and the number of polynomials of degree at most d is $1 + \sum_{k=0}^d N_k$. Results of Section 5 now easily give the number of solutions for s with denominator of degree d when $L \leq d \leq n$:

COROLLARY 6.4 *For $L \leq d \leq n$, the number of solutions for s with denominator of degree d is $N_{d-L} \left(1 + \sum_{k=0}^{d-L-e_s} N_k\right)$.*

PROOF. Let $E_d = \{(f_1, f_2) : f_1 \in \text{Ann}(s)^\times : |f_1| = d\}$. From Corollary 5.6 or Corollary 5.11, we have $f \in E_d$ if and only if $f_1 = \varphi'\mu_1 - \varphi\mu'_1$ where (i) $|\varphi'| = d - L$ and (ii) $\varphi = 0$ or $|\varphi| \leq d - L - e_s$, which yields the stated result. \square

6.2 Non-Vanishing Annihilating Polynomials

We consider the following problem: let $a \in D$ be arbitrary and suppose that $\mu_1(a) = 0$. Find a solution $\xi = (\xi_1, \xi_2)$ such that $\xi_1(a) \neq 0$ and ξ_1 has least degree among solutions with first component not vanishing at a . We begin with a pseudo-geometric example.

EXAMPLE 6.5 *Let $n \geq 2$ and $s = s_0, \dots, s_{1-n} = 1, 0^{n-1}$. Then $e_s = n - 1 > 0$ and $\nabla_s = 1$, so $\text{MP}(s) = \{\varphi'x : \varphi' \in D^\times\}$ by Corollary 5.4. Thus all minimal polynomials of s vanish at 0. However $g = (x^n + 1, x^{n-1})$ is a solution for s and $g_1(0) \neq 0$. We will shortly see that $\min\{|f_1| : f \text{ is a solution for } s, f_1(0) \neq 0\} = n$, so that $|g_1|$ attains this minimum.*

We can assume that s is non-trivial and $L \geq 1$, for otherwise $\mu_1 \in D^\times$ vanishes nowhere. Put $\text{Ann}(s)^{(a)} = \{f_1 \in \text{Ann}(s) : f_1(a) \neq 0\}$. Any polynomial of degree n which does not vanish at a annihilates s , so that

$$L^{(a)} = \min\{|f_1| : f_1 \in \text{Ann}(s)^{(a)}\}$$

is well-defined and $L \leq L^{(a)} \leq n$. We put $\text{MP}(s)^{(a)} = \{f_1 \in \text{Ann}(s)^{(a)} : |f_1| = L^{(a)}\}$. Example 6.5 shows that $L^{(a)} - L$ can be arbitrarily large. As usual, μ' is obtained as in Algorithm 4.12.

COROLLARY 6.6 *If $\mu_1(a) = 0$ then $\mu'_1(a) \neq 0$.*

PROOF. Proposition 4.20 yields $\mu_2\mu'_1 - \mu_1\mu'_2 \in \mathbb{F}^\times$, so $\mu'_1(a) \neq 0$ (and $\mu_2(a) \neq 0$). \square

Using Proposition 5.3, Theorem 5.10 and Corollary 6.6, we can now solve the problem posed at the head of this subsection.

THEOREM 6.7 (Cf. [14, Proof of Theorem 3.7]) *Let $n \geq 1$, s_0, \dots, s_{1-n} be a sequence over D , $e = n + 1 - 2L_n$ and $M = \max\{e, 0\}$. If $\mu_1(a) = 0$ then $L^{(a)} = L + M$. In fact $\xi_1 = x^M\mu_1 - \mu'_1 \in \text{MP}(s)^{(a)}$ and $\xi_2 = x^M\mu_2 - \mu'_2$.*

PROOF. If $n = 1$ and $\mu_1(a) = 0$ then $a = 0$ and $e = 0$; $\xi_1 = \mu_1 - \mu'_1 = x - 1 \in \text{MP}(s)$ satisfies $\xi_1(a) \neq 0$ and $\xi_2 = s_0 = \mu_2 - \mu'_2$, so ξ is the required solution and $L^{(a)} = L + M$.

If $n \geq 2$ and $e \leq 0$ then $\xi_1 = \mu_1 - \mu'_1 \in \text{MP}(s)$ so $L = L^{(a)}$ and $\xi_2 = \mu_2 - \mu'_2$ by Lemma 5.13. Also $\xi_1(a) \neq 0$ by Corollary 6.6 and so ξ is the required solution.

Now let $n \geq 2$ and $e > 0$. We have $L + e = n + 1 - L \leq n$ since $L \geq 1$. We first show that $L^{(a)} \geq L + e$. Let $f_1 \in \text{Ann}(s)^{(a)}$, $f = (f_1, f_2)$, $m = \langle f, \mu \rangle$ and $m' = \langle f, \mu' \rangle$. From Proposition 5.3 or Theorem 5.10 we have $\nabla_s f_1 = m'\mu_1 - m\mu'_1$ where $|m'| = |f_1| - L \geq 0$ and $|m| \leq |f_1| + L - n - 1$. If $|f_1| + L - n - 1 < 0$ then $m = 0$, $\nabla_s f_1(a) = m'(a)\mu_1(a) = 0$ and $f_1 \notin \text{Ann}(s)^{(a)}$ for a contradiction. Hence $|f_1| \geq n + 1 - L = L + e$ and $L^{(a)} \geq L + e = L + M$.

To see that $L^{(a)} \leq L + M$, let $\xi_1 = x^M\mu_1 - \mu'_1$ which has degree $L + M$. We have $\xi_1(a) = -\mu'_1(a) \neq 0$ by Corollary 6.6. We claim that $\xi_1 \in \text{MP}(s)^{(a)}$. We have $|1| = 0 = |\xi_1| + L - n - 1$, so by Lemma 5.2 or Lemma 5.9 we have $\xi_1 \in \text{Ann}(s)^{(a)}$ and $L^{(a)} \leq |\xi_1| = L + M$.

Finally, we verify that $\xi_2 = x^M\mu_2 - \mu'_2$. Put $\varphi' = x^M$ and $\varphi = 1$. If s is pseudo-geometric, Lemma 5.5 applies since $|\varphi| = 0 \leq L - 1$ and $0 \leq M \leq n - 1$. Hence $\xi_2 = x^M\mu_2 - \mu'_2 = x^M\mu_2$. Suppose that s is essential. We have $0 \leq M \leq n + 1 - 2L \leq n - L$ since $L \geq 1$, so that Lemma 5.13 applies and $\xi_2 = x^M\mu_2 - \mu'_2$ in this case too. \square

Theorem 6.7 yields the following simple extension of Algorithm 4.12.

ALGORITHM 6.8 (Cf. [14, Algorithm 3.2])

Input: $n \geq 1$, $a \in D$ and sequence $s = s_0, \dots, s_{1-n}$ over D .

Output: Solution ξ for s such that $\xi_1 \in \text{MP}(s)^{(a)}$.

[Algorithm 4.12 (input : n, s ; output : μ, μ');

if $\mu_1(a) \neq 0$ then $\xi \leftarrow \mu$ else $\xi \leftarrow x^{\max\{n+1-2|\mu_1|, 0\}}\mu - \mu'$;

return ξ .]

Table 2: Algorithm 4.12 for 0, 1, 1, 0, 0, 1, 0, 1 over \mathbb{F}_2

s	Δ_1	e_s	μ	μ'
	—	—	$(1, 0)$	$(0, 1)$
0	0	1	$(1, 0)$	$(0, 1)$
0, 1	1	2	$(x^2, 1)$	$(1, 0)$
0, 1, 1	1	−1	$(x^2 + x, 1)$	$(1, 0)$
0, 1, 1, 0	1	0	$(x^2 + x + 1, 1)$	$(1, 0)$
0, 1, 1, 0, 0	1	1	$(x^3 + x^2 + x + 1, x)$	$(x^2 + x + 1, 1)$
0, 1, 1, 0, 0, 1	0	0	$(x^3 + x^2 + x + 1, x)$	$(x^2 + x + 1, 1)$
0, 1, 1, 0, 0, 1, 0	1	1	$(x^4 + x^3 + 1, x^2 + 1)$	$(x^3 + x^2 + x + 1, x)$
0, 1, 1, 0, 0, 1, 0, 1	1	0	$(x^4 + x^2 + x, x^2 + x + 1)$	$(x^3 + x^2 + x + 1, x)$

EXAMPLE 6.9 Table 2 gives the iterations of Algorithm 4.12 (implemented using [3]) for the sequence s over \mathbb{F}_2 of [14, Table I]; we have omitted Δ'_1 as it is the constant 1. We see that s is essential, $e = e_s = 1$ and $\mu_1(0) = 0$. Theorem 6.7 implies that $L^{(0)} = L + e = 5$ and Algorithm 6.8 gives $\xi = x^e \mu + \mu' = (x^5 + x + 1, x^3 + x^2)$.

REMARKS 6.10 (i) Algorithm 6.8 is simpler than [14, Algorithm 3.2], e.g. it does not include tests on μ'_1 . It also computes μ_2 . Corollary 6.12(ii) below, a version of which was stated without proof in [14], was used to justify Algorithm 3.2, loc. cit. In Algorithm 3.2, loc. cit. the polynomial μ'_1 is initialised to 1 as in [7] rather than 0; see Remark 4.13.

(ii) The original motivation of [14]: let $a = 0$ and ξ_1^* be the reciprocal of ξ_1 . Since $\xi_1(0) \neq 0$, $|\xi_1^*| = |\xi_1| = \delta$ say, $(\xi_1^* \cdot \xi^*)_i = (\xi_1 \cdot \xi)_j$ where $j = 1 - n + \delta - i$, and $\delta + 1 - n \leq i \leq 0$ if and only if $\delta + 1 - n \leq j \leq 0$. Hence if $1 \leq \delta < n$, ξ_1 and the first δ terms $s_0, \dots, s_{1-\delta}$ uniquely determine the last $n - \delta$ terms $s_{-\delta}, \dots, s_{1-n}$ if and only if $1 \leq n - \delta < n$, ξ_1^* and the last $n - \delta$ terms $s_{1-n}, \dots, s_{\delta-n}$ uniquely determine the first δ terms $s_{\delta-n+1}, \dots, s_0$.

We can also construct an element of $\text{MP}(s)^{(a)}$ by extending s by one term.

COROLLARY 6.11 (Cf. [14]) Let $s = s_0, \dots, s_{1-n}$, $\mu_1 \in \text{MP}(s)$ and $\mu_1(a) = 0$. Suppose that $e = e_s \geq 1$. Put $t = s, s_{-n}$ where s_{-n} is chosen so that $\Delta(\mu_1; t) \neq 0$. If ν_1 is obtained as in Theorem 4.9 then $\nu_1 \in \text{MP}(s)^{(a)}$.

PROOF. Let $\Delta_1 = \Delta(\mu_1; t)$. Since $e \geq 1$, $\nu_1 = \Delta'_1 x^e \mu_1 - \Delta_1 \mu'_1 \in \text{MP}(t)$ from Theorem 4.9 and $|\nu_1| = n + 1 - L = L^{(a)}$ by Theorem 6.7. Further, $\nu_1(a) = -\Delta_1 \mu'_1(a) \neq 0$ by Corollary 6.6 and since $\text{Ann}(t) \subseteq \text{Ann}(s)$, $\nu_1 \in \text{MP}(s)^{(a)}$. \square

For the Example of Table 2, $\Delta_9 = 1$ requires $s_9 = 0$ and we obtain $\nu = \xi$ as before.

COROLLARY 6.12 Let $s = s_0, \dots, s_{1-n}$ be a sequence over \mathbb{F} , μ, μ' be as usual and $m = \langle f, \mu \rangle$, $m' = \langle f, \mu' \rangle$. If $a \in \mathbb{F}$, $\mu_1(a) = 0$ and $M = \max\{e_s, 0\}$ then

- (i) $\text{Ann}(s)^{(a)} = \{\varphi'\mu_1 - \varphi\mu'_1, |\varphi'| \neq 0, |\varphi| \leq |\varphi'| - e_s, \varphi(a) \neq 0\};$
- (ii) $\text{MP}(s)^{(a)} = \{f_1 \in \text{Ann}(s)^{(a)} : |m'| = M, |m| \leq |f_1| + L - n - 1, m(a) \neq 0\};$
- $$= \{\varphi'\mu_1 - \varphi\mu'_1 : |\varphi'| = M, |\varphi| \leq M - e_s, \varphi(a) \neq 0\}.$$

PROOF. (i) This is a restatement of Corollary 5.4 or Corollary 5.11. (ii) We have $\nabla f_1 = m'\mu_1 - m\mu'_1$ and $f_1 \in \text{Ann}(s)$ if and only if $|m'| = |f_1| - L$ and $|m| \leq |f_1| + L - n - 1$. Also $|f_1| = L + M$ from Theorem 6.7 since $f_1 \in \text{MP}(s)^{(a)}$. Similarly if $g_1 = \varphi'\mu_1 - \varphi\mu'_1$ then $g_1 \in \text{Ann}(s)$ if and only if $|\varphi'| = |g_1| - L$, $|\varphi| \leq |\varphi'| - e_s$ by Lemma 5.2 or Lemma 5.9 and $|g_1| = L + M$ by Theorem 6.7. \square

For Example 6.9, $e_s = 1$ and so $\text{MP}(s_0, \dots, s_{-7})^{(0)} = \{x\mu_1 + \mu'_1, (x+1)\mu_1 + \mu'_1\}$.

References

- [1] Berlekamp, E. R. *Algebraic Coding Theory*. Series in Systems Science. McGraw Hill, New York-Toronto, 1968.
- [2] Cheng, U. On the Continued Fraction and Berlekamp's Algorithm. *IEEE Transactions on Information Theory*, 30:541–544, 1984.
- [3] Cocoa Team. *A System for Doing Computations in Commutative Algebra*. Available at <http://cocoa.dima.unige.it>, Version 5.0.
- [4] Gustavson, F. G. Analysis of the Berlekamp-Massey linear feedback shift-register synthesis algorithm. *IBM J. Res. Dev.*, 20:204–212, 1976.
- [5] Lidl, R. and Niederreiter, H. *Finite Fields. Encyclopedia of Mathematics and its Applications*. Addison-Wesley, Reading, 20, 1983.
- [6] MacWilliams, F. J. and Sloane, N. J. A. *The Theory of Error-Correcting Codes*. North Holland, Amsterdam, 1977.
- [7] Massey, J. L. Shift-Register Synthesis and BCH Decoding. *IEEE Trans. Inform. Theory*, 15:122–127, 1969.
- [8] Mills, W. H. Continued Fractions and Linear Recurrences. *Mathematics of Computation*, 29:173–180, 1975.
- [9] Niederreiter, H. Sequences with Almost Perfect Linear Complexity Profile. Advances in Cryptology — Eurocrypt '87 (D. Chaum, W.L. Price, Eds.). *Lecture Notes in Computer Science*, 304:37–51, 1987.
- [10] Northcott, D. G. Injective Envelopes and Inverse Polynomials. *J. London Math. Soc.*, 8:290–296, 1974.

- [11] Norton, G. H. On the Minimal Realizations of a Finite Sequence. *J. Symbolic Computation*, 20:93–115, 1995.
- [12] Norton, G. H. On Shortest Linear Recurrences. *J. Symbolic Computation*, 27:323–347, 1999.
- [13] Norton, G. H. The Berlekamp-Massey Algorithm via Minimal Polynomials. *math.ArXiv: 1001.1597*, pages 1–22, 2010.
- [14] Salagean, A. An Algorithm for Computing Minimal Bidirectional Linear Recurrence Relations. *IEEE Trans. Info. Theory*, 55:4695–4700, 2009.
- [15] Welch, L. R. and Scholtz, R. A. Continued Fractions and Berlekamp’s Algorithm. *IEEE Trans. on Information Theory*, 46:19–27, 1979.